1-1-2017

When Cyber Systems Crash: Attitudes Towards Cyber Utilization And Security

Nicholas L.K. Tar
Nova Southeastern University, tarnicho@yahoo.com

When Cyber Systems Crash:
Attitudes Towards Cyber Utilization And Security

by

Nicholas Lebbea Kernyuy Tar

A Dissertation Presented to the
College of Arts, Humanities, and Social Sciences of Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy

Nova Southeastern University
2017

Nova Southeastern University
College of Arts, Humanities, and Social Sciences

This dissertation was submitted by Nicholas L. K. Tar under the direction of the chair of the dissertation committee listed below. It was submitted to the College of Arts, Humanities, and Social Sciences and approved in partial fulfillment for the degree of Doctor of Philosophy in Conflict Analysis and Resolution at Nova Southeastern University.

Approved:

February 24th, 2017
Date of Defense

Elena P. Bastidas R
Elena Bastidas, Ph.D.
Chair

Urszula Strowińska - Zanko
Urszula Zanko, Ph.D.

Solomon Losha, Ph.D.

.

6/8/2017
Date of Final Approval

Elena P. Bastidas R.
Elena Bastidas, Ph.D.
Chair

Dedication

I dedicate this thesis to my wife, Susan Tar and my sons, Nicholas Tar, Jr., Nathan Tar, and Noah Tar. The decision to dedicate this thesis to my wife and children was an easy one because they were not only the source of my inspiration but most importantly the engine that propelled me forward when things got tough. My wife Susan, a law school graduate herself knew the importance of higher education and supported me enthusiastically from start to finish. During my course work years, she was the one driving me to and from the airport to attend residential institutes at NSU Florida, and for that, I am very grateful. Right in the middle of the program the birth of our three lovely boys, whom we fondly call "the three wise men," and their night cries was the raison d'etre for which, I worked hard to secure a better future for them. I pray that this doctoral degree should act as a symbol of encouragement to my kids to cherish and love education and also work hard to achieve in their lives what their parents were not able to achieve. I love you all dearly.

Acknowledgement

After years of rigorous scholarship in the Ph.D. program, I have come to this singular point of acknowledging those whose unrelenting support guided me through this incredible academic journey that culminated in writing and defending this doctoral thesis. Words of thanks can only do scant justice to my dissertation chair, Dr. Elena Bastidas, and committee members Dr. Urszula Zanko and Dr. Solomon Losha whose continuous support, positive criticism, and immense knowledge helped me get to the point of defending this thesis. Their expertise in quantitative methodology though sometimes grueling created a contagious force that compelled me to hone my statistics knowledge and meet the standards required to conduct research in the quantitative tradition.

This thesis represents not only my work in the library and at the keyboard but exhibits a milestone of years of assiduous study and research at the College of Arts, Humanities, and Social Sciences at Nova Southeastern University. My experience and intellectual pursuit at NSU has been nothing short of amazing. As a doctoral student at NSU, I was given unique opportunities for intellectual growth, and I took advantage of them culminating to this final research masterpiece. For that, I remain eternally grateful to all my professors at NSU.

The support, love, and encouragement of my late dad, Simon Nyuyki Tar and late uncle Wilfred Nsai Nassir has not only been an everlasting engine of strength but has engraved in me the constant desire to work hard and stretch beyond the limits of my imagination. Although self-proclaimed as the least intelligent child in a family of five, my dad always prayed for my success and believed that I was destined to either be a priest or a doctor. I am proud that I am both of those things today, a doctor of philosophy

and a member of the universal priesthood. I know he is deeply happy in his heavenly home knowing that his son Nicholas Tar has run his academic race to the finish.

The prayerful best wishes and wise counsel of my mom Irene B. Tar; brothers Emile L. Tar, Joseph Brian, Hermann B. Tar and Emmanuel Ngam; sisters Yvonne Fanka and Camilla Y. Tar; nieces, nephews and aunt Rev Sister Mary Fidelis; and especially my in-law Henry Fanka, and uncles Shufai America Edward Mancho, Bernard Fonlon, Jr., Joseph Musa, and Gregory Wirba cannot escape my memory, and for that, I remain infinitely indebted.

Throughout these years I have learned that just as there are those who build tools and those who use them I am inclined towards creating the tools used in cutting-edge scientific and technological research. This thesis presents the lessons learned in working as a Linux cloud security engineer at both the USCIS Douglas Development Center and the FCC Incentive Auctions Program. My supervisors and co-workers in these environments have not only been exceptional IT engineers, managers, directors, and architects but inspirational in their dedication to IT excellence and security.

I am particularly thankful to Venkat Veeramneni and Fadi Harake, technocrats and entrepreneurs at Nuvitek. Their dedication to excellence in IT engineering has not only been contagious but has also instilled in me an ever growing desire to work hard to build the expertise needed to deploy secure and healthy applications to the cloud.

I am equally indebted to the group of engineers (database, network, and Unix/Linux) and project managers at the Incentive Auctions Program at FCC with whom I work every day. Their dedication to IT excellence has been commendable. Worthy of mention are the following Linux/Unix engineers: Tonyio Afagbegee, Kumar Nainala,

Rayudu Konanki, David Dugard, Pugazhendhi Selvaraju, Welf Dixon, Jay Black our program manager, and Erik Scheibert, our architect. Bernie Beale and Zena Smith's friendship also cannot be forgotten.

Finally, I say thank you for the support I received from friends and IT professionals like Daniel Aboyewa and Chuma, Eddy Mayi, Estella Muma, and Divine Anye. May God bless all those whose prayers and support made this possible.

Table of Contents

List of Tables vii

List of Figures x

List of Acronyms xi

Abstract xiii

Chapter 1: Introduction and Justification of the Study 1

Background Relevance of the Study 8

Problem Statement 12

Purpose of the Study 14

IT Risk Management Overview 17

Research Questions 19

Hypotheses 20

Theoretical Framework 22

Nature of the Study 25

List of Key Variables for the Study 26

Definition of Terms 27

Description and Operation of Variables 30

Dependent variable. 30

Some methods used to breach cybersecurity networks. 31

Independent variables. 34

Control variables. 36

Description of Methodology, Data Collection, and Analysis 38

Level of Measurement of Variables 38

Population of the Study 39

Sampling 39
Assumptions 40
Scope and Delimitations Inferences 41
Limitations in the Study 42
Significance of the Study 44
Conclusion 44
Chapter 2: Review of Literature 46
Introduction and Restatement of the Research Problem 46
Synopsis of Themes and Theories 50
Emergent Themes from Literature 52
Preview of Major Sections of this Chapter 55
Literature Search Strategy Used in the Study 56
Theories and Their Applications to Security 58
Social Learning Theory and Cybersecurity 59
General Deterrence and Rational Choice Theories of Cybersecurity 63
Technology Acceptance Model and Cybersecurity 64
Socio-Technical Systems Theory and Cybersecurity 67
Summary of Theories and Their Application to Security 70
Literature Review Related to Key Variables and Concepts 71
The Phenomena and Definition of Cybercrime 73
Attitudes Towards Cyber Utilization 78
Conclusion 84
Chapter 3: Methodology 85

Introduction 85
Research Design and Rationale 88
Methodology 91
Sampling and Sampling Procedures 93
Procedures for Recruitment, Participation, and Data Collection 95
Pilot Survey Study 97
Data Analysis and Interpretation Following the Chi-Square Correlation Analysis Model 99
The Chi-Square Formula Used in the Analysis of the Observed and Expected Frequencies 101
Justification for Using Chi-Square Statistics in the Research 102
Unit of Analysis 103
Operationalization and Manipulation of Variables 103
Explanation and Manipulation of the Information Security Variable 103
Justification for Including the Information Security Variable in the Analysis 105
Explanation and Manipulation of the Attitudes Towards Internet Use Variable 105
Justification for Including Attitudes Towards Internet Use in the Analysis 106
Explanation and Manipulation of the Cybersecurity Awareness Training Variable 107
Justification for Including Security Awareness Training in the Analysis 108

Explanation and Manipulation of the IT Savvy Variable 109
Justification for Including the IT Savvy variable in the Analysis 110
Explanation and Manipulation of the Type of Transaction Variable 111
Justification for Including Type of Transaction in the Analysis..... 111
Explanation and Manipulation of the Financial Loss Variable 112
Justification for Including Financial Loss in the Analysis..... 113
Explanation and Manipulation of the Level of Education Variable 113
Justification for Including Level of Education in the Analysis 114
Explanation and Manipulation of the Gender Variable 114
Justification for Including Gender in the Analysis 115
Explanation and Manipulation of the Age Variable 116
Justification for Including Age in the Analysis 117
Explanation and Manipulation of the Residence Variable 117
Justification for Including Residence in the Analysis..... 118
Conclusion 117
Chapter 4: Data analysis and Presentation..... 120
Introduction..... 120
Description of the Sample Used in the Study 120
Demographic and Descriptive Data 121
Analysis of the Sample in Relation to the Responses on the Research Instrument 123
Analysis and Interpretation of the Cross-Tabulations 130
Cross-Tabulation of Cybersecurity Awareness Training and Concern

for Security 132
Cross-Tabulation of Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity 137
Cross-Tabulation of Type of Transaction One Uses the Internet for and Concern for Security 142
Cross-Tabulation of Concern for Security and Associated Financial Cost Incurred from Cyber breach 148
Cross-Tabulation of Level of Education and Concern for Internet Security 152
Cross-Tabulation of Gender and Concern for Internet Security 157
Cross-Tabulation of Age and the Importance of Internet Security 161
Cross-Tabulation of Residence Location and the Importance of Internet Security 165
Conclusion 169
Chapter 5: Discussion and Implications of the Study 171
Introduction 171
A Summary Discussion of Findings of the Hypothesis Tested 171
Analysis of the Results That Did Not Reveal a Relationship in with Literature 176
Analysis of the Results that had a Weak Relationship with Literature 181
Conclusion and Implication of the Findings 184
Implication of the findings vis-à-vis systems theory and holistic cybersecurity awareness 184

Implication of findings vis-à-vis best practice and social change. 186

Implications of findings vis-à-vis crisis management and conflict resolution..... 188

Recommendations for Action and the Way Forward 189

References..... 192

List of Tables

Table 1. Age of Participants....121
Table 2. Gender Description....122
Table 3. Level of Education Description....122
Table 4. Residence Location Description....123
Table 5. Participants Indicating IT Savvy....124
Table 6. Participants Indicating Internet Security an Important Factor....125
Table 7. Concern for Security Rating....125
Table 8. Internet Most Used for Which Transactions....126
Table 9. Internet Transaction Determines Concern for Internet Security....126
Table 10. Participants Indicating Cybercrime or Scamming Victim....127
Table 11. Type of Cybercrime Experienced....128
Table 12. Participants Indicating Cybersecurity Training....129
Table 13. Participants Indicating Cybersecurity Awareness Training as Important....129
Table 14. Type of Cybersecurity Awareness Training Considered Important....130
Table 15. Case Processing Summary Table of Cybersecurity Awareness Training and Concern for cybersecurity....133
Table 16. Contigency Table of Cybersecurity Awareness Training and Concern for Security....134
Table 17. Pearson Chi-square Statistics of Cybersecurity Awareness Training and Concern for Security....134
Table 18. Lambda Test of Association of the Variables....137

Table 19. Case Processing Summary Table of Level of User's Considering Themselves as IT Savvy and Concern for Cybersecurity 138
Table 20. Contingency Table of Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity 139
Table 21. Peason Chi-square Statistics of Concern for Security and Cyber User's Considering Themselves as IT Savvy 142
Table 22. Case Processing Summary Table of Type of Transaction One uses the Internet for and Concern for security 143
Table 23. Contingency Table of Type of Transaction One Uses the Internet for and concern for security 145
Table 24. Pearson Chi-square Statistics of Type of Transaction One Uses the Internet for and Concern for Security 147
Table 25. Gamma Test of Association of the Variables 147
Table 26. Case Processing Summary Table of Associated Financial Cost Incurred due to Cyber breack and Concern for Security 148
Table 27. Contingency Table of Associated Financial Cost Incurred due to Cyber breach Cyber breach and Concern for Security 149
Table 28. Pearson Chi-square Associated Financial Cost Incurred due to Cyber breach and Concern for Security 152
Table 29. Case Processing Summary Table of Level of Education and Concern for Cybersecurity 153
Table 30. Contingency Table of Level of Education and Concern for Cybersecurity 154

Table 31. Pearson Chi-square Statistics of Level of Education and Concern for Cybersecurity 156
Table 32. Case Processing Summary Table of Gender and Concern for Cybersecurity 158
Table 33. Contingency Table of Gender and Concern for Cybersecurity 159
Table 34. Pearson Chi-square Statistics of Gender and Concern for Cybersecurity ... 161
Table 35. Case Processing Summary Table of Age and Concern Cybersecurity 162
Table 36. Contingency Table of Age and Concern for Cybersecurity 163
Table 37. Pearson Chi-square Statistics of Age and Concern for Cybersecurity 165
Table 38. Case Processing Summary Table of Residence Location and Concern For Cybersecurity..... 166
Table 39. Contingency Table of Residence Location and Concern for Cybersecurity 167
Table 40. Pearson Chi-square Statistics of Residence Location and Concern for Cybersecurity 169
Table 41. Table of Results That Are Significant in Chi-square but Low in Their Lambda or Gamma Effect..... 176
Table 42. Table of Results That Were Not Statistically Significant in Chi-square 176

List of Figures

Figure 1. Chi-square statistics formula. 102

Figure 2. Chi-square statistics formula expanded. 102

Figure 3. Cybersecurity awareness training and concern for security. 135

Figure 4. Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity. 140

Figure 5. Type of Transaction you use the Internet for and Concern for Security. 146

Figure 6. Concern for security and Associated Financial Cost Incurred due to Cyber breach. 151

Figure 7. Bar chart of level of education and concern for cybersecurity. 156

Figure 8. Gender and the concern for cybersecurity. 160

Figure 9. Age and concern for cbersecurity. 164

Figure 10. Residence location and concern for cybersecurity. 168

List of Acronyms

AARP	American Association of Retired Persons
ATM	Automated Teller Machine
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity and Availability
CSI	Computer Security Institute
CV	Control Variable
DC	District of Columbia
DCAR	Department of Conflict Analysis and Resolution
DDoS	Distributed Denial-of-Service
DL	Data Loss
DV	Dependent Variable
FBI	Federal Bureau of Investigation
FL	Financial Loss
FIPS	Federal Information Processing Standard
GDT	General Deterrence Theory
IAP	Incentive Auctions Program
IBM	International Business Machines
IC3	Internet Crime Complaint Center
IDS	Intrusion detection systems
IP	Internet Protocol
IPS	Intrusion protection systems
IT	Information Technology

IV	Independent Variable
MRH	Main Research Hypothesis
MRQ	Main Research Question
NIST	National Institute of Standards and Technology
NSA	National Intelligence Agency
NTIA	National Telecommunications and Information Administration
RCT	Rational Choice Theory
RQ	Research Question
SLT	Social Learning Theory
SOX	Sarbanes-Oxley Act of 2002
SP	Special Publication
SPSS	Statistical Package for the Social Sciences
SQ	Sub-Question
STST	Socio-Technical Systems Theory
TAM	Technology Acceptance Model
UN	United Nations
US	United States

Abstract

This research focused on examining attitudinal differences of Internet utilization and security with the objective of understanding the relationships that cyber usability have with cybercrime and then determine best practices needed to promote the secure use of the Internet. The research was designed as a quantitative study that used judgment sampling to survey 433 cases to explain the relationship that exist between cyber utilization and security. To achieve this objective, research questions and hypothesis were designed to guide the analysis. Cross tabulation analysis was used to compare the dependent and independent variables while Chi-square, Lambda and Gamma statistical tests were used to verify the relationship and identify statistical significance of the relationship. The findings revealed that while variables like being IT savvy, amount of financial loss, education, age, gender and residence location did not have evidence of a relationship with security, research participants had concern for secure cyber use and thought that cybersecurity awareness training and type of transaction conducted on the Internet were associated to security even though the strength of each relationship was weak. The study highlighted the damaging effects of cybercrime and recommended that cyber users should embrace best practice principles as they browse the Internet and utilize cybersecurity awareness training as an important function of secure IT utilization.

Chapter 1: Introduction and Justification of the Study

Information technology systems such as the Internet are extremely beneficial to people all over the world, especially university students who depend on them to conduct research and in some cases attend online classes. Due to the Internet, major transformations have happened in the way humans communicate, work, play, learn, do business, and engage with others economically, politically, educationally, culturally, and socially. IT systems assist businesses with the ability to operate better, as well as improve customer relationships and stakeholder values (Setia, Venkatesh, & Joglekar, 2013).

Constant technological innovations are helping businesses drive efficiency and also increase business value daily (Caniëls, Lenaerts, & Gelderman, 2015). Daily research and forecasting trends in the financial markets and supply chain management processes needed for daily life are made possible by computer systems (Zhang, van Donk, & van der Vaart, 2011).

Although the benefits of the Internet abound, it is possible with the passage of time for humanity to quickly start to forget or even take for granted the developments and life improvements acquired from technology given that technology and in particular the Internet are now common facts of life. When we think of the benefits of the Internet and remember that just over 20 years ago the Internet was almost unheard of among the general population and was only available to a small and specialized group of academicians, scientists, military, and in government laboratories, we cannot but appreciate it more as its expansion has been exponential.

Nonetheless, as more people use the Internet subtle and sometimes drastic problems associated with its use—especially those related to cyber-attacks, cybercrime, data security, and privacy—continue to be on the rise (Arlitsch & Edelman, 2014).

Due to all these threats, President Barack Obama has cautioned that cyber threat is one of the most serious economic and national security challenges the United States faces (Schmidt, 2010). In support of President Obama's pronouncement, the National Institute of Standards and Technology (NIST, 2011) has stated that developed countries like the United Sates have emphasized the importance of cybersecurity both for national and business security. Cybercrime is dangerous and can create political blackmail and sabotage as proven by the Russian hacking scandal on the 2016 US presidential elections.

The dangers of a cyber-attack are real, thus explaining why the U.S. government, the military, and the intelligence community have taken significant steps to build intrusion detection systems with the capability to defend unwanted intruders to their networks and also monitor adversarial systems with the purpose of identifying and dismantling threats before they are deployed (Schmidt, 2010).

In a bid to protect these cyber systems, the National Security Agency (NSA) and the intelligence community has built and used cyber intelligence detective satellites designed to monitor and perform reconnaissance operations on adversarial networks. These detective satellites are used to monitor and identify malicious cyber plots and also track terrorist activities for eventual capture. Examples of high target terrorist whom the US government captured through the aid of cyber intelligence detective technologies include Osama bin Laden, Anwar al-Awlaki, Mohammed Emwazi alias Jihadi John, and other high-value terrorists.

The fact is that, although Internet use is beneficial to users in many ways, its security concerns also abound thus highlighting a dangerous and urgent threat that should be resolved or at least contained. As increasing numbers of people in the United States and around the world, both in the private and public sectors, rely on cyberspace for everyday communication and business, protection of these systems and infrastructure rests in the domain of cybersecurity (Aitoro, 2010b), and striking a balance between reaping the benefits of the Internet with a security guarded attitude is critical.

The primary motivator of a cyber-attack is theft of data, intellectual property, or financial assets for personal gain. Therefore, personal data, financial data, educational data, health data, and national security data must be guarded against this threat. Since financial assets are particularly guarded against cybersecurity threats, colleges and university systems have become favored targets as they store data similar to banks (Musil, 2014).

It is now commonplace to hear that most university's financial, administrative, employment-related records, library records, and intellectual property related records have been attacked. All of these incidences have put university students on a high cybersecurity alert. An example of a cyber-attack on a university system was the 2014 University of Maryland's sophisticated cyber-attack in which, sensitive and personally identifiable information of more than 300,000 faculty members, staff, and students were stolen (Musil, 2014).

Discussion on cybersecurity regularly dominates technology discourse in media outlets and the news in the U.S. and many industrialized countries around the world. In 2013 the average cost of managing cybersecurity-related incidents for 60 cyber-based

organizations in the U.S. was 11.56 million dollars. In Germany, the price for the same number of agencies in the same year was 7.56 million dollars, Japan 6.73 million dollars, France 5.19 million dollars, United Kingdom 4.72 million dollars, and Australia 3.67 million dollars (Ponemon Institute, 2013). These statistics demonstrate the seriousness of a cyber-attack and highlight the fact that the threat is not just technological but equally economical as it could quickly render a company or country bankrupt due to the high cost incurred from managing and addressing cyber-attacks.

Considering the pertinence of the context of this study, it is; therefore, appropriate to use the words of the renowned Chinese general Sun Tze spoken over 2,500 years ago to underscore the importance of this subject. Over 2,500 years ago general Sun Tzu asserted, "Know the enemy, and know yourself, and in a hundred battles you will never be in peril" (Tzu, 2005, p. 125). These words are right in military warfare and equally valid in cyber warfare since knowing the enemy that threatens information technology effectiveness is a critical first step that helps engineers and cyber users design and uses secure systems.

The enemy here is primarily the hackers who are able and ready to exploit security loopholes as well as authorized cyber users who in some cases are described as "the weakest link in the cybersecurity chain" (Sasse & Flechais, 2005, p. 13). Users with bad and nonchalant attitudes towards security are as dangerous as hackers. Therefore, identifying the adversary is a critical first step in combating cyber-attacks, and knowing the type of role that Internet users' attitudes play towards the occurrence of cybercrime creates a better platform needed to address the cybercrime problem. It is important to note that computer security is not merely a discourse on technology as it is also a

discussion on the personnel that utilizes these systems, the processes that rely on this technology, and the programmatic policies that determine how people should interact with these systems. Therefore, human actions can either help enhance the security and smooth functioning of cyber systems or unfortunately, mar their effectiveness thus causing damage worth a lot of money.

Information security threats and cyber-crime have overlapping meanings in this research and to underline such overlap, it is necessary to define both terms. According to Newman (2009), cybercrime is a situation in which, a computer or a network is used as a tool, a target, or just a hub for criminal conduct.

Though this includes the subject of information security and ways to prevent or detect malicious intruders from gaining unwanted access to information assets, it also encompasses much larger situations like using computers to commit a crime, especially "traditional" offenses. On the other hand, information security, according to NIST SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800- 60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 (as cited in Kissel, 2013), is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (p. 94).

Other phrases used to describe cybersecurity breaches include cyber warfare which, denotes a deliberate computer-based assault from one state to the other to cause damage (Vijayan, 2010), as well as cyber-espionage which, deals with stealing sensitive government digital information (Harris, 2010).

Careful examination of the above terms reveals an intrinsic connection between cybercrime and information security breach since the occurrence of cyber-crime

demonstrates the use of computers or networks as tools, targets, or simply hubs for criminal activity mostly in unauthorized circumstances. Therefore, the presence of cyber-crime indicates a breach or violation of information security systems.

Although cyber-crime incidents or information security violations are mostly caused by the malicious actions of hackers, cyber users' carelessness and unconcerned attitudes to security, unfortunately, act as stepping stones that are used by hackers to cause damage to a cyber infrastructure worth millions of dollars. Therefore, highlighting this issue, by developing security awareness programs and creating practical ways that help Internet users stay vigilant to security while using the Internet, will contribute substantially to maintaining data integrity, confidentiality, and availability.

The seriousness of the cyber threat problem is real as unauthorized access to data on the Internet has reached unprecedented levels, thus posing significant challenges to users (Eloff & von Solms, 2000; Schultz, Proctor, Lien, & Salvendy, 2001). Everyone who uses the Internet has a stake in this game, especially software developers who write software as well as cyber users who use the Internet for business and other activities.

It is a sad reality that Internet users who are the beneficiaries of technology are seen as "the weakest link in the chain" (Sasse & Flechais, 2005, p. 13) of system security and as a result are used by hackers to breach security. Kevin Mitnick, a renowned hacker, proves this point when he professes the ease with which, hackers crack passwords by tricking users through social engineering techniques. Such an example indicates a major security loophole in users that must be addressed if we expect to make any progress in successfully securing systems (Sasse & Flechais, 2005).

The desire for people to protect themselves and their assets is not new to humanity. Security has always been an important part of human life since people's safety, and possessions are always at risk from deliberate attacks or accidental damage and the same holds when dealing with data assets. The ever growing need and use of technology, especially the Internet for various purposes, underline the need for people and organizations to protect their electronic assets since experience shows that hackers are always around and ready to do harm.

Although literature indicates that information technology professionals continually try to improve and enforce information security, more work is needed as cyber breaches are still rampant. Although people and especially businesses allocate enormous financial resources towards the safety of their systems, purchasing and deploying such security assets, do not automatically secure systems as many users are careless about security and feel that a cyber breach is far from affecting them. Such wishful thinking is dangerous for if cyber users continue to neglect security mechanisms like virus checkers, password management or email encryption, and other security tools, any effort to protect information systems is futile (Sasse & Flechais, 2005).

The fact is that cyber users' attitudes toward security play a critical role in either helping enforce IT security or not. If users ignore the possibility of a connection between their Internet use attitudes and cyber threats, and continue to exhibit careless cybersecurity attitudes by indiscriminately disclosing their passwords, failing to encrypt confidential messages, continuing to switch virus checkers off, and failing to acknowledge the possibility that their cybersecurity use attitudes can put data assets at risk, security breaches will continue to occur.

Attackers need to exploit just a single error to inflict severe damage. What is worrisome is that most Internet users continue to do the same things and expect different results. If Internet users admit that they are the weakest link in the security chain and fail to improve their attitudes towards information security, attackers will continue to exploit human factor loopholes and attempt to breach systems (Mitnick & Simon, 2003).

As chapter one proceeds, the background and relevance of the study are presented by summarizing literature relevant to the topic and presenting gaps in the literature that will possibly be filled by the research. Chapter one also presents the problem statement of the research in a way that highlights the importance of engaging in the research. By doing this, the purpose of the study is highlighted as well as the methodology used to analyze the problem statement adequately.

Also, the research questions and hypotheses are provided and analyzed using data gathered from the survey. Research variables are also explained, and key terms are defined. Research limitations are also discussed, thus highlighting the significance and importance of the research in knowledge development.

Background Relevance of the Study

In this modern world of technology, and in particular the past decade, reliance on information technology (IT) for daily business activities and competitiveness has reached alarming levels in all countries (Grant & Royle, 2011). Very few people if any in Western society are left out from the full effects and use of information technology and the Internet. With advancement in globalization, educational, economic, political, military, legal, and social institutions progressively rely on automated systems and information technology for their energy and delivery services.

This dependence poses security risks when all these services are coordinated by Internet-based systems which, in themselves are vulnerable due to software, hardware, and human-related security factors. Although large amounts of valuable and sensitive data are continually processed, stored, and retrieved from these IT systems, there is the enormous risk of abuse as unauthorized players strive daily to steal such data for personal gain (Bisong & Rahman, 2011).

Global economic and political settings, technological infrastructure, and socio-cultural changes continue to create changing environments for establishments such as universities and businesses that depend on cyber systems for efficient delivery of their services. All these human and non-human factors increase the number of threats undergone by cyber assets and an isolationist and nonchalant attitude towards these threats cannot be the norm (Loch, Carr, & Warkentin, 1992). Thes threats call for constant monitoring of IT systems as 93% of large companies, and 87% of small businesses continually report security breaches regularly (Price Waterhouse Cooper, 2013).

Computer and information security scholars have indicated the need for Internet users to incorporate cybersecurity techniques in their daily attitudes towards cyber use. The result of ignoring this exultation leads to vulnerable systems that only pose a security risk to business data (Straub & Welke, 1998). This focus on IT security is critical to companies in both the public and private sector as literature indicates data compromise affecting more than 200 million consumers regularly (Garrison & Ncube, 2011).

In the modern world, IT security management is not a new concept as data is vital for business (Susanto, Almunawar, & Tuan, 2012). With the mass usage of the Internet,

the importance of data security cannot be overemphasized. Therefore, organizations should implement controls that protect their IT systems and measure and monitor the depth of the threats they face (Carter, Phillips, & Millington, 2012).

In the information technology industry, four key aspects of information are protected and preserved. These are availability, integrity, authenticity, and confidentiality (Parker, 1998). Availability means protecting information to make it accessible for a particular purpose. Integrity means protecting information so that it is complete, whole, and unchanged. Authenticity means protecting information so that it is valid and genuine. Confidentiality means protecting information so that it is only disclosed to authorize individuals (Parker, 1998).

A significant concern in information security management is the issue of effective remediation of vulnerabilities and damages caused by attacks and systemic failures. Despite this real problem, the literature indicates that more attention is still geared towards technological approaches to solving the cyber threat problem (Besnard & Arief, 2004) rather than employing a socio-technical methodology that encompasses the technical and the human aspects of IT (Dhillon & Backhouse, 2000).

Though technical configurations are critical in addressing some of the security issues, the human factor input is equally important considering that technology is designed, implemented, operated, secured, and maintained by people (Rasmussen, 1994; Reason, 1997). Therefore, regardless of the strength and sophisticated design of technical configurations to protect and secure networks, information security failures caused by human actions create vulnerability loopholes that are exploited by hackers for their gain (Bishop, 2002).

Cybercrime and cyber-attacks are a real problem in this epoch than ever before (Arlitsch & Edelman, 2014). In the past few decades, computer crimes were primarily committed by disgruntled employees who willfully inflicted physical damage on the computer itself. Hacking was practiced by software developers who performed penetration testing and ethical hacking drills by writing malicious software and self-replicating programs to interfere with security for testing, hardening, and learning purposes. Hacking now has gradually evolved to involve widespread activities from hackers who make money by willfully hacking into systems for their gain.

With increased cyber-attacks and data theft in this computer age, businesses now dedicate an average of 40% of their annual IT budget to fight cyber-attacks (Lo & Chen, 2012). Social scientists now spend enormous amounts of research hours writing about the importance of data security as well as the factors that may or may not explain such activity. Among these factors, the roles of human and organizational factors have been studied through the lens of many disciplines. Some of these studies focus on areas like cognitive engineering, computer science, human factors engineering, information systems and security, management sciences, systems dynamics and complexity sciences.

Although these disciplines examine the effects of human attitudes on information systems, the complexities inherent in these activities call for continuous research to cover the existing gaps (Cresswell & Hassan, 2007; Dhillon & Backhouse, 2000; Furnell, 2007; Schultz, 2005).

The justification of this study lies in the fact that it provides an empirical test emanating from existing literature and survey data on the relationship between users' attitudes and the security of the Internet. The existing literature on the subject is scanty,

and research has not been able to design an effective solution to the cyber threat problem as seen from the increasing number of cyber-attacks all over the world. Nonetheless, the literature indicates a relationship that needs to be analyzed.

This study intends to overcome methodological limitations from previous studies by not depending only on literature but going a step further to gather firsthand data from cyber users through a survey. The questions on the questionnaire are designed to collect accurate information on the topic but not in an open-ended fashion. This methodology ascertains greater visualization and simultaneous analysis of survey data, thus providing stronger statistical influence. The approach also draws its strengths from the analysis of limitation and risk factors gathered from the statistical method used in the study. By incorporating these risk factors and analyzing them, greater insight is formed.

Problem Statement

This study is designed to focus on university students in the Washington, DC, area to understand the relationship that exists between attitudes of cyber user's towards technology adoption and the security of the Internet. Having an understanding of this relationship is critical to the study because cyber-attacks not only occur through actions from hackers but also because of attitudes of authorized cyber users. Internet use is good, but ignorance of its safety concerns is dangerous as one mistake can damage an entire system. Therefore, Internet users are encouraged to understand the effects that their attitudes have on the security of their IT systems and develop a safety conscious attitude while using the Internet.

The importance of the Internet as a repository of data needed for human enterprising cannot be denied, thus explaining why increasing numbers of people have

embraced daily Internet usage as an integral part of daily living. Internet use for educational and research purposes is noticeable in many domains of life, and although physical libraries still exist as a symbol of research and knowledge, the proliferation of virtual libraries makes research even easier, thus making Internet use an unavoidable part of student life.

Despite all these use cases, great danger lurks around the corner as hacking activities continue to rise. The IC3 public service announcement entitled "Cyber-related Scams Targeting Universities, Employees, and Students" underlines this problem and indicates that on January 13, 2015, an FBI warning was issued cautioning university students to beware of fictitious ‘work-from-home' scams (Federal Bureau of Investigation, 2015).

A study conducted by Price Waterhouse Cooper indicates that the number of detected cyber-attacks in the U.S. skyrocketed in 2014 and increased 48% from 2013 (White, 2014). This increase in cyber-attacks have prompted companies to report over 2,800 data breaches that affect well over 543 million records (Romanosky, Hoffman, & Acquisti, 2014).

According to scholars, 42.8 million cyber-attacks occurred in 2015 amounting to roughly 117,339 attacks each day (Bennet, 2014) and the combined costs of U.S. government and corporate IT security programs amounted to $15 billion yearly (Executive Office of the President of the United States, 2013), thus creating an urgent crisis for cybersecurity and emergency management professionals. Cybersecurity engineers, cyber users, and IT professionals must take these attacks seriously and increase research focused on determining how to deal with the cyber threat problem

either through training, theory development, defensive systems development, change of policy, and most importantly, changes of attitude from the users' end. The fact is that cybercrime is real and can potentially generate damage of enormous proportions if not carefully handled.

Understanding and dealing with the issue of cybersecurity is critical as the Internet continues to play a fundamental role in people's lives. The Nielsen data underscores this point, stating that in 2011 over 274.2 million Americans used the Internet with a certain probability that even greater numbers would join the bandwagon of Internet users. Representing this growth in monetary terms, in 2011 alone Americans spent over $256 billion on retail and travel-related purchases online (Palis, 2012).

These numbers highlight the importance of educating cyber users on how to use the Internet securely. The intent of this research is to understand the relationship that cyber users attitudes have on the occurrence of cybercrime, and by so doing highlight the importance of security for daily cyber use and also lay the groundwork for improved cybersecurity research through cybersecurity awareness training and information sharing.

Purpose of the Study

The research focusses on employing sample survey to examine attitudes of university students towards Internet utilization and security in order to understand the type of relationships that exists between cyber utilization and the occurrence of cybercrime. This knowledge would determine best practices needed to promote data confidentiality, availability and integrity.

Although much literature has explained the interaction between humans and computer systems (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014), a limited

focus is devoted to explaining the relationship that exists between cyber users attitudes and cybercrime. This notwithstanding, the very limited attempts to explain factors that affect the safe or unsafe use of cyber systems are written in technical language that is mostly incomprehensible to regular cyber users (Trček, Trobec, Pavešić, & Tasič, 2007). Technology scholars must find effective ways of promoting technology using simple language that explains the technical functions of technology without compromising security. Such a move would help cyber users create a better attitude adopting and using technology.

While isolating and discussing the relationship that exists between poor cyber users' attitudes and cybersecurity breaches, the analytical reasoning that accounts for potential intervening variables necessary to mitigate the possible harm that could occur as a result of a cyber breach is broadened. This approach helps to prevent the possibility of porosity in explaining the relationship that exists between cyber users' attitudes towards security and the occurrence of cybercrime. Also, this research is pertinent because it contributes to developing a systematic and scientific basis for good policy action that would inform and educate cyber users on safe ways to use the Internet.

The increasing number of cyber-attacks and vulnerabilities generate costly consequences to cyber users and corporations. News outlets always publish reports that highlight the cost of cyber-attacks to businesses around the world. Most of these reports highlight the billions of dollars lost to computer theft, fraud, and abuse. (Power, 2002). An example of such a report is the 2002 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey on Computer Crime and Security Survey. According to this survey, 90% of respondents from government and corporations acknowledged having

experienced a cyber-attack leading to financial losses that could total approximately $455,848,000 (Power, 2002).

Another 2008 report from the Computer Security Institute and the Federal Bureau of Investigation survey of data from 522 information security practitioners from corporations in the United States indicated that an average loss per participant was $288,618 caused by all types of computer security incidents (Richardson, 2008).

In May 2014 IBM sponsored the Ponemon Institute to conduct research on cyber breach incidents on 61 organizations in the United States, and the report indicated that in 2014 alone, 44% of incidents of cyber-attacks involved a malicious or criminal attack, 31% emerged from employee or users negligent, and 25% emanated from some system glitch that includes information technology and some business process failures (Ponemon Institute, 2014). From these breaches, the most costly involved malicious actions against the organization which, amounted to $246 per capita data breach. Next to this were system glitches or some human error amounting to a cost of $171 and $160 per capita data breach respectively. All of these numbers amounted to a total yearly cost ranging from $688,250 to $23.1 million to companies (Ponemon Institute, 2014).

When post data breach costs like help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services, and regulatory interventions were calculated, data show that companies incurred an additional $1.60 million in expenses added to the already massive costly data breaches. Added to all of this is the $3.03 million lost business costs which, include abnormal turnover of customers, increased customer

acquisition activities, reputation losses, and diminished goodwill (Ponemon Institute, 2014).

The study also sought to discover if the relationship between users' attitudes towards the security of the Internet could be used as an early indicator of a vulnerability that could account for a possible cybersecurity breach. Nhara (1996) theorizes early warning as an information system that can provide indicative data that could be used to forecast the emergence of a crisis or a possible cyber breach. Such an assertion from Nhara highlights the fact that cyber breaches can be predicted and as a result, examining cyber users' attitudes towards cybersecurity is important as it helps raise awareness and highlight early warning signs that could degenerate to a cyber crisis (1996).

IT Risk Management Overview

Risk management as construed in this research focuses on the gross adverse effects of the existence of vulnerabilities in consideration of the probability and the impact of occurrence. This risk management framework instituted by the National Institute of Standards and Technology (NIST) is necessary for the study because it highlights the importance of cybersecurity by explaining the nature of risks that exist in cyber environments with the aim of indicating how such risk could be managed and remediated through risk assessment (NIST, 2016).

The goal of incorporating risk assessment in the study is because it gives cyber users the ability to understand the risk associated with their attitudes towards Internet use and gives them the method needed to manage such risk in a way that helps them address issues before they become a reality. Risk assessment ensures that the information the system contains is confidential, available when needed and not randomly changed.

Risk management and assessment help cyber user's select cost-effective security controls that meet their needs. Risk management should then be shaped by the business objective (NIST, 2016). From a business perspective, users must identify the services that promote their business objective, locate the ones that are most critical to the business, assess the risk they face and address the most critical risks first to prevent an attack.

It is important to note that computer and cybersecurity management programs are not only designed for a group of selected users but rather everyone who uses the Internet for those who fail to practice good cybersecurity destroy the efforts of those who do and as a result render the whole security effort futile.

Risk management here involves three processes that work together to enforce security in an IT environment. These are risk assessment, risk mitigation, and risk evaluation. All of these factors are necessary for an effective risk management program and most incorporate risk assessment processes, risk mitigation steps, and finally, risk assessment measures. Risk assessment and management is not unique to the information technology industry and as a result permeates decision-making in all areas of human existence (NIST, 2016).

The risk management framework's knowledge should be incorporated into the regular training curriculum that must be taken by all cyber users in an organization. This structure begins by categorizing the information system following the National Institutes of Standards and Technology Special Publication, NIST SP 800-60 and the Federal Information Processing Standard, FIPS 199 guidelines. After categorizing, the next step would be to select the security controls and set a baseline following NIST SP 800-53. After that, the security control is implemented using NIST 800-18 guidelines. After

implementing the controls, the framework assesses the security checks using NIST 800-53A as a guide and developing a security assessment report using NIST 800-30. Next, the system is authorized, and a plan of action and milestones for the environment is created which, helps remediate any future vulnerabilities identified. To conclude, the framework enables a regular monitoring mechanism on the implemented security controls using NIST SP 800-137 (NIST, 2016).

Research Questions

This study explains the relationship that exists between cyber utilization and concern for cybersecurity to understand what accounts for the occurrence of cybercrime. To accomplish this objective research questions were identified:

RQ1. Is there a relationship between the users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity?

RQ2. Is there a relationship between the users considering themselves as IT savvy and their level of concern for cybersecurity?

RQ3. Is there a relationship between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity?

RQ4. Is there a relationship between amount of financial loss experienced due to cyber breach and level of concern for cybersecurity?

RQ5. Is there a relationship between the Internet user's educational level and their level of concern for cybersecurity?

RQ6. Is there a relationship between the Internet user's gender and their level of concern for cybersecurity?

RQ7. Is there a relationship between the Internet user's age and their level of concern for cybersecurity?

RQ8. Is there a relationship between the Internet user's residence location and their level of concern for cybersecurity?

Hypotheses

Hypotheses are used in research to answer research questions and define relationships between research variables and that was the case in this research. To adequately examine the relationships that exists between cyber utilization and security the below hypotheses were developed.

Hypothesis H1: There is a significant association between the Internet users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity.

Hypothesis $H0_1$: There is no significant association between the Internet users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity.

Hypothesis H2: There is a significant association between Internet users considering themselves as IT savvy and their level of concern for cybersecurity.

Hypothesis $H0_2$: There is no significant association between Internet users considering themselves as IT savvy and their level of concern for cybersecurity.

Hypothesis H3: There is a significant association between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity.

Hypothesis $H0_3$: There is no significant association between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity.

Hypothesis H4: There is a significant association between the amount of financial loss incurred due to cyber breach and level of concern for cybersecurity.

Hypothesis $H0_4$: There is no significant association the amount of financial loss incurred due to cyber breach and level of concern for cybersecurity.

Hypothesis H5: There is a significant association between the educational level of the cyber user and their level of concern for cybersecurity.

Hypothesis $H0_5$: There is no significant association between the educational level of the cyber user and their level of concern for cybersecurity.

Hypothesis H6: There is a significant association between the gender of the cyber user and their level of concern for cybersecurity.

Hypothesis $H0_6$: There is no significant association between the gender of the cyber user and their level of concern for cybersecurity.

Hypothesis H7: There is a significant association between the age of the cyber user and their level of concern for cybersecurity.

Hypothesis $H0_7$: There is no significant association between the age of the cyber user and their level of concern for cybersecurity.

Hypothesis H8: There is a significant association between the residence location of a cyber user and their level of concern for cybersecurity.

Hypothesis $H0_8$: There is no significant association between the residence location of a cyber user and their level of concern for cybersecurity.

Theoretical Framework

Information assurance—unlike many other traditional disciplines like psychology, sociology, and criminology though in existence for many years—assumed not only striking recognition but also a particularly unique usage after the ratification of the Sarbanes-Oxley Act of 2002 which, responded to a highly visible wave of corporate malfeasance (Cegielski, 2008). This recent emphasis on information assurance after the Sarbanes-Oxley Act justifies why an extensive literature on the subject is still scant.

The emerging and growing threat posed by cyber-attacks highlights a rare but necessary urgency in cybersecurity theory development as the world is becoming increasingly complex, dynamic and unpredictable. Computer scientists, social psychologists, criminologists, conflict resolution practitioners and other researchers are currently looking at ways to adequately explain these emerging crimes as existing models and methods for conflict resolution are particularly challenged in the face of these trends. These trends happen so fast such that conflict resolution practitioners have to play catch up to this reality as their solutions are rapidly becoming ineffectual (Coleman, 2011).

Due to the fluid and changing dynamics of technology, effective literature development has to borrow from many disciplines to adequately explain the many

components of information security. Therefore, chapter two of the study concentrates on scrounging from research that lies at the intersection of information technology, social psychology, sociology, criminology, and human behavior to explain the relationship between cybersecurity, human attitudes, and cyber usability.

To adequately understand the connection that usability has on the security of the Internet, human error emerges as an important factor that needs to be analyzed (Senders & Moray, 1991). Such analysis will clarify the complex relationships and underlying triggers that initiate action or inaction as it relates to cybercrime.

Cybersecurity breaches are unwanted realities that indicate the vulnerabilities present in technology systems as efficient and secure mediums of data transmission. These vulnerabilities indicate that information security has to be an integral part of software development and promoted by both the engineers and users.

At the heart of most cyber-attacks are human weakness, human error, and the dynamics of human attitude. Technological loopholes, as well as human limitations, are exploited by cyber criminals for their personal gain. To initiate a theoretical framework that would help develop ways to address the problem of cybercrime, scholars have started developing human error frameworks, theories, and models (Senders & Moray, 1991).

What is not very clear is whether these human error structures can be used to conduct a comprehensive personal usage analysis of crisis in the cybersecurity industry or at least provide a structure around which, new human investigative techniques can be designed. At the same time, if all these concerns could be explained easily, this endeavor would not be necessary and would also eliminate the need to create yet another error

framework. Therefore, the question that needs to be answered is ‘how do you identify and apply an adequate framework for your use case'?

The best way to approach this issue would be to examine theories postulated by scholars on this subject (Shappell & Wiegmann, 2001). From a glance, this approach seems daunting if one would have to examine each and every theory considering that the issue of usability, human attitudes, and human error has been discussed for decades and many human error models, theories, and frameworks have been developed (Senders & Moray, 1991).

The issue here is that not all of these theories, models, and frameworks are relevant in adequately explaining the present study's focus, thus explaining why the challenge would be to identify and analyze just those that are significant to this study.

The effort here would then be to approach this topic in a focused fashion, limiting attention to examining a smaller and more manageable collection of cyber usability theories that have a relationship with cyber user's attitudes on Internet security. With this approach, four relevant theories are identifiable with their unique advantages and disadvantages (Shappell & Wiegmann, 2001; Wiegmann, Rich, & Shappell, 2000). These are social learning theory, general deterrence and rational choice theories, technology acceptance model, and the socio-technical systems theory (Shappell & Wiegmann, 2001). In chapter two these theories are explored for their contributions in explaining cybersecurity while focusing on isolated frameworks that characterize each theory to the extent that they are relevant to analyze user's attitudes towards Internet security.

Nature of the Study

Constant changes in technological know-how and input from many variables make it challenging for cybersecurity researchers and engineers to develop a comprehensive solution for the cybersecurity problem. For this reason, cybersecurity theory is continually being developed to meet the changing nature of technology and the threats they face, thus explaining why this study is designed to be associational, not causational.

Since cyber-attacks evolve daily and involve a plethora of players, it is challenging to develop a single solution or explanation to every cyber incident. The intention here then is that more clarity should be brought to the subject by understanding the type of relationship that exists between the variables. To do this, questions will be raised that are focused on challenging scholars to expand research in the intersection of information technology, conflict resolution, and social psychology. Through this research, the phenomenon becomes more familiar, and new insights are acquired that are needed in theory development.

To bring more clarity to the subject the potential parallels and relationships that exist between the variables are examined to see how that relationship shapes literature. Another important component of this research is the literature review. Although literature development related to this subject is ongoing, the extant literature is tapped and expanded. Critical to the study is the questionnaire which, has been designed to capture specific responses that will help clarify the relationship that exists between variables, thus helping to expand theory.

The research method for this study is quantitative because the relationship between variables and the validation or invalidation of research hypothesis is being examined (Denzin, 2012). Qualitative methodology can also be used to explore a problem, case, or group through surveys, interviews, and observations of participants (Bansal & Corley, 2011). Qualitative methodology was not fitting for this study because participants were neither observed nor interviewed.

Another methodology which, could have been used is mixed-method. Mixed-method is used when combining participants' experiences and empirical data to determine the relationship and differences between identified variables (Yin, 2013). Since the study only focused on the relationship between variables collected from participants' responses to the questionnaire, a mixed-method in the study was not incorporated.

List of Key Variables for the Study

To adequately understand and find ways to make Internet use safe for students in the Washington, DC, area of the United States, research variables would have to be listed, defined, and analyzed. Such definitions will indicate the factors to watch for when analyzing the relationship that exists between cyber users' attitudes and cybersecurity.

From the standpoint of topic design and approach, cybersecurity is the variable that was tested using input from cyber users. For that reason, cybersecurity is the dependent variable while the independent variables comprised of cyber users' attitudes towards security, the amount of financial loss, type of cyber-attacks experienced, and cybersecurity training. Control variables included age, gender, the level of education, and residence location.

Definition of Terms

Cybersecurity. Cybersecurity also called IT security, centers on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction (Kissel, 2013).

Information security threats. This term broadly means any possible harm or damage resulting from the inappropriate misuse or abuse of protected information assets (Haley, Laney, Moffett, & Nuseibeh, 2006). Further, information security threats are situations that may result in an information system compromise to cause an adverse effect on business operations, business assets, and individuals such as disclosure or unauthorized access of confidential information through social engineering and phishing (Ryan, Mazzuchi, Ryan, Cruz, & Cooke, 2012).

Information security practice. Information security practice involves the following:

> Individuals' information security risk management behavior involving two aspects: the adoption of security technology and safety conscious care behavior related to computer and Internet usage. The former is related to the use of security software and features such as Anti-virus software, Anti-spyware, and a pop-up blocking function. The latter refers to security compliance behavior in using a computer and the Internet, such as the use of a secure password and frequency of making a backup copy. (Rhee, Kim, & Ryu, 2009, p. 818).

Cyber-crime. According to Newman (2009), cybercrime is defined to be a situation in which, a computer or a network is used as a tool, a target, or just a hub for criminal conduct.

Hacker. The word hacking connotes the act of illegally breaking into computer networks and the Internet to steal data for personal gain, and those who personally commit themselves to this kind of illegal activity are called hackers (Howard, 1997; Hutchison, 1997; Rasch, 1996; Stoll, 1985; Taylor, 1998).

Attitude. Attitude is "a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor" that sometimes leads to action (Eagly & Chaiken, 1993, p. 1; Ferguson & Bargh, 2007).

IT savvy. IT savvy as used in the study refers to someone who is knowledgeable and proficient in using technology especially computers or having practical knowledge of how to use computers.

Computing experience/knowledge. Computing experience/knowledge (CE) has been defined as the users' knowledge and expertise in computers, the Internet, and information security (Rhee et al., 2009).

Cyberspace. The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Joinson, 2001; Kissel, 2013).

Data breach. A data breach is an unauthorized access to secure information or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information (Adebayo, 2012; Romanosky et al., 2014).

Information assurance. Information assurance constitutes the measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality (Kissel, 2013).

Access. According to the National Institute of Standards and Technology (NIST SP 800-32) (as cited in Kissel, 2013) and Harris (2013), access is the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Cloud computing. According to Harris (2013) and Kissel (2013), cloud computing is a computer model that enables on-demand network access to a shared pool of configurable computing capabilities or resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Critical infrastructure. According to the Committee on National Security Systems (CNSSI-4009) (as cited in Kissel, 2013), critical infrastructure is the systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Enterprise risk management. Enterprise risk management is a comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives (Kissel, 2013; Harris, 2013).

Intrusion detection. According to the National Institute of Standards and Technology (NIST SP 800-32) (as cited in Kissel, 2013) and Harris (2013), intrusion detection is the process and methods for analyzing information from networks and information systems to determine if a security breach or safety violation has occurred.

Bugs. According to the Webster's New World Dictionary of American English, a bug is "an unexpected defect, fault, flaw, or imperfections" (Neufeldt & Guralnik, 1991, p. 182). In programming jargon, "errors" are known as "bugs." The process of finding bugs before program users do is called debugging which, starts after the code is first written and continues in stages as code is combined with other units of programming to form products like operating systems or applications.

Description and Operation of Variables

Dependent variable

Cybersecurity. According to the Committee on National Security Systems (CNSSI-4009) (as cited in Kissel, 2013) and Fuchs, Pernul, and Sandhu (2011), the concept of cybersecurity as used in this study refers to any attempts to secure cyber systems due to the impending cyber-attack committed with the aid of the Internet or similar IT or telecommunications mediums. These would include social engineering breaches, malware, software based violations, application attacks, network based breaches, wireless threats and vulnerabilities, physical security breaches, and vulnerabilities (Kissel, 2013).

According to Brenner (2004), cybercrime which, is the area of cybersecurity we are focusing on is any criminal activity that involves the Internet, a computer system, or computer technology. It could also be said to be the illegal use of computers and the Internet for personal gain. Types of cybercrime are things like identity theft, phishing, social engineering techniques, and others. Cybercrime is also sometimes called hacking which, originated from the illegal act of modifying a program by changing the code itself to serve an unlawful purpose. Cybersecurity and cybercrime would be used

interchangeably in this study, depending on the circumstance under discussion. Cybersecurity is operationalized in this study as the level of concern for cybersecurity an individual has.

Some methods used to breach cybersecurity networks

Social engineering. This variable in the study is construed to be an attack in which, the hacker uses deception and trickery to convince unsuspecting cyber users to provide sensitive data or to violate security guidelines (Taylor & Nufryk, 2014). There are two types of social engineering attacks. These are semantic and syntactic.

Semantic social engineering. These are exploits that target the security flaws in the people operating the computer rather than the machine itself and can be done using human-based or computer-based methods. In the context of this study, asyntactic and semantic social engineering will be defined as exploits aimed at manipulating the social and psychological behaviors of cyber users with the intention of obtaining private user information to illegally and fraudulently access data for personal benefits (Barrett, 1997; Schneier, 2000).

Syntactic social engineering. These are exploits related to the software or network operating logic or vulnerabilities such as loopholes in software, denial of service, and difficulties with cryptographic algorithms (Schneier, 20001). In the context of this study syntactic, social engineering will be defined as exploits related to fundamental security failings such as malware and smurfing.

Malware. This is one of the most common threats that affect computers today. In the study, malware is described to be malicious code or unwanted software that infect computer systems and cause them to operate in undesirable ways. According to Taylor

and Nufryk (2014) and Harris (2013), malware is insidious and difficult to remove from the system under attack because it can come in many forms which, sometimes are difficult to identify and eradicate even with the most sophisticated vulnerability protection tool.

Malware is, therefore, not monolithic in nature as it comes in different forms and methods, thus making it difficult to kill. Identifying the various types of malware and how they operate puts one in a better state to fight their infection and prevent them from infecting the system. Some forms of malware or malicious code attacks are viruses, worms, adware, spyware, Trojan horses, rootkits, logic bombs, botnets, ransomware, armored viruses, and much more (Taylor & Nufryk, 2014).

***Software-based threats*.** Besides attacks that trick the human components of information systems like social engineering attacks and those that highlight the dangers of malicious code, there exist attacks that focus directly on the software elements of the system (Taylor & Nufryk, 2014). In the study, these are identified as attacks that target the operating system and other computer software systems. These forms of attacks can severely cripple the operations of the computer, and therefore, it is important that cyber users recognize these types of attacks and be able to guard against them. Some of such attacks are password attacks and backdoor attacks (Taylor & Nufryk, 2014).

Application attacks. These forms of attacks are described in the study to be software attacks that target web-based systems or other client-server applications (Taylor & Nufryk, 2104). These are dangerous because they do not only limit themselves to applications, web servers, users, and other back-end systems but can also attack the application code itself. When this happens authentication breaches could occur, as well as

customer impersonation, information disclosure, source code disclosure or tampering, and severe network breaches. Some of these forms of attacks are cross-site scripting attacks, zero-day exploits, attachment attacks, buffer overflow, and much more (Taylor & Nufryk, 2014).

Network-based threats. These forms of attacks are described in the study to be attacks that hijack networks which, are the lifeblood of systems, thus cutting networks from connecting with others to produce information or enable communication (Taylor & Nufryk, 2014). These forms of attacks can bring business systems down, thus causing significant damage worth millions of dollars. Some of these are IP port scanning attacks, eavesdropping attacks, man-in-the-middle attacks, replay attacks, social network attacks, DoS attacks, and session hijacking attacks, and much more (Taylor & Nufryk, 2014).

Wireless threats and vulnerabilities. These forms of attacks are identified in the study as attacks that focus on wireless systems and cause damage to internal and wireless networks (Taylor & Nufryk, 2014). It is no news that wireless networks are everywhere nowadays and protecting devices against wireless vulnerabilities is important in shielding sensitive data from unauthorized access. Wireless security is, therefore, important as it secures these networks from unwanted access. Some of these attacks are rouge access points, evil twins, jamming, bluejacking, bluesnarfing, war driving, packet sniffing, and much more (Taylor & Nufryk, 2014).

Physical threats and vulnerabilities. When threats to information systems are considered, virtual threats are mostly the focus. Though dangerous in themselves, physical threats are equally dangerous. These forms of attacks in the study are described to compose and affect the physical components of the network and the facilities that

contain the systems (Taylor & Nufryk, 2014). What is significant from these forms of attacks is the fact that physical resources are equally important when talking about information security. Although it is important to keep attackers away from networks, it is equally important to shield them from stealing, compromising, or destroying the hardware in which, these systems run. Some of the physical threats to guard against can be internal, external, natural, or human-made (Taylor & Nufryk, 2014).

Independent variables

Attitudes towards Internet use. Attitude here explains an established way of thinking or feeling about something which, is reflected in behavior or action. A positive attitude exudes positive behavior while a negative attitude projects negative behavior. Attitude towards Internet use then explains a cyber user's operational inclination towards Internet use and its associated activities (Smith, Caputi, & Rawstone, 2000).

A cyber user’s disposition towards using the Internet and its associated activities determines whether the user would use the Internet securely or not. If a cyber user has a positive attitude towards cybersecurity training for example, that attitude would be seen in how securely the user would use Internet. According to Garland and Noyes (2005), the more confident a cyber user is towards accessing and using the Internet securely, the more positive his or her attitude would be towards using the Internet, thus enhancing security in the system.

Since one's attitude towards something predisposes action, attitude towards Internet usability as utilized in the study describes the positive or adverse effects that cyber users' attitudes have on the security of the web (Smith et al., 2000). Learning about the relationship that exists between one's attitude and the security of the Internet is

important because a user's inability to use the Internet securely contributes to cyber exploitation which, in most cases is dangerous to businesses or the victims.

Internet security is a big issue in the U.S. today, and that explains why news outlets regularly broadcast incidences of cyber-attack. In June of 2013 news outlets presented a cascade of reports released by NSA contractor Edward Snowden concerning government surveillance programs. These revelations opened new wounds and highlighted concerns about how best to preserve citizen's data in the digital age.

Though data security is necessary for protecting cyber assets against cyber-attacks, cyber surveillance in itself is problematic as people are not sure of where the balance lies between data security and cyber surveillance. Striking a balance between data security and confidentiality with cyber surveillance is another topic that needs careful study.

IT savvy. Savvy as verb means to know or to understand something. Savvy is sometimes used as an adjective to indicate that someone is experienced, knowledgeable or well-informed about something. Savvy could also be used as a noun to indicate practical understanding, shrewdness or intelligence towards something (Neufeldt, V., & Guralnik, D. B., 1991). IT savvy as used in the study refers to someone who is knowledgeable in using information technology systems or having practical knowledge of how to use computers.

The financial cost incurred from cybercrime. This variable helped the researcher find out whether the amount of money incurred from a cyber-attack would determine the victims' keenness to cybersecurity (Acquisti, Friedman, & Telang, 2006). One would think that anyone who suffers a significant amount of monetary loss as a result of a

cyber-attack might pay attention to security more than someone who incurs a smaller amount of financial loss as a consequence of a cyber-attack. Although this might seem reasonable, such a conclusion cannot be drawn from sentiments but rather from survey data which, this research presents.

Cybersecurity awareness training. The very basis for any cybersecurity training is to assist a participant to become aware of the cyber threats that exist and also give a cyber user the tools necessary to guard against those threats (Eminağaoğlu et al., 2009). This notion, therefore, creates the assumption that people who have taken cybersecurity training might be better Internet users than those who have not. In an academic discourse, such a sweeping statement must be backed by facts, and survey data would help the researcher make an informed argument about this issue.

Type of Internet transaction. This variable helped the researcher determine whether the kind of business conducted on the Internet has any relationship with one's keenness to security. This is important as it clarifies the assumption that people who use the Internet for financial transactions care about security more than those who use the Internet for less sensitive activities.

Control variables

Age. The issue of age can seem unnecessary and inconsequential when talking about information security, but that might quickly change if one starts to look at what age group is comfortable accessing and using information systems. This question is the very reason why age was introduced in the study.

The reason age is brought to the study is to find out if certain age groups find it easier to use the Internet securely than others and whether such willingness to use the Internet securely has a relationship on Internet use or not.

The issue then would be that although all students use the Internet, younger college students might be more knowledgeable dealing with information security than seniors. This is important in this research as the study findings would indicate where resources should be allocated to advance security.

Gender. This variable is relevant to the study as it helped show from the survey if one gender has more concern for Internet security than the other and why. Such knowledge also helped propose how to align resources when dealing with addressing cybersecurity (American Psychological Association, 2006, pp. 1-2).

The level of education. This variable is important in the study as it indicates if a cyber user's level of education has a relationship with their concern for security or not (Hornsby, 2006). Since the level of education might align to age, the research paid attention to survey data to see if there is any disparity concerning being a victim of cybercrime among young students and older students. The issue of whether carelessness has something to do with age and educational qualification was also explained when analyzing this variable.

Residence. The researcher's intent with this variable was to know if a cyber user's place of residence has any relationship with cybersecurity awareness. This knowledge is important because it clarifies the assumption that cyber users who live in urban areas and access the Internet easily are more familiar with Internet security than cyber users live in

rural areas and might not have easy access to the Internet. Survey data informed these presuppositions and shaped theory.

Description of Methodology, Data Collection, and Analysis

This study explored attitudinal differences in Internet use and security with the objective of understanding the relationship that cyber users' attitudes have on an individual's level of concern for cybersecurity. Cyber-attacks have been occurring and causing damage to networks for a long time, thus explaining the necessity to understand what factors account for cyber-attacks. In an attempt to understand cybercrime and the connection it has with cyber users attitudes, the research collected and analyzed data from regular cyber users through a survey. Survey questions were designed to capture the relationship that cyber users' attitudes have on cybersecurity not from the perspective of a cause and effect finding but rather from a relationship finding process. In addition to using the survey as the primary source of data collection, existing literature was also used to analyze the data.

Level of Measurement of Variables

The standard of measurement of variables is significant as it revealed the type of relationship that exists between the values assigned to the attributes for each variable. Such analysis helped determine how to interpret data obtained from each variable. Looking at the nature of the survey questions, most of the variables were nominal with the possibility for some to be ordinal during measurement and data manipulation.

Survey questions were designed to extract targeted information from the participants. This method was intentional as it helped eradicate answers that strayed from

the research objective. Survey questions were not only categorized but mostly demanded ‘yes' or ‘no' answers, thus underlining their nominal nature.

Population of the Study

Internet use has become a fundamental and unavoidable part of daily living. This is because almost all aspects of the human experience depend on the Internet either for business, research, healthcare, and other activities. This dependence on the Internet is even more significant in educational environments. Now in the world as a whole and the U.S. in particular almost all degree programs have a fundamental link to the Internet either for research, administrative, or business purposes.

It is recorded that approximately 86% of students in the United States depend upon and use the Internet for their education compared to 59% of the general population (Jones, 2002). These numbers even get higher when looking at samples from specific universities. Fortson, Scotti, Malone and Del Ben (2007) assert that during a similar study, 90% of their survey respondents acknowledged using the Internet on a daily basis. This data encouraged the researcher to limit the population for this study to students ranging from 18 years and older. This age group covers students from college level up to the graduate and doctoral levels.

Sampling

In this research, students of all genders attending universities around the Washington, DC, metro area were sampled. Participants had to fall within the ages of 18 years and older and actively use the Internet. The method was to design a questionnaire and upload on SuveyMonkey for university students around Washington, DC, to freely

and willingly participate in the survey. The expectation was to receive a total of 433 cases.

In research, a sample can be defined as "that finite part of a statistical population whose properties are studied to gain information about the whole" (Neufeldt & Guralnik, 1991, p. 1187). In the case of human interaction, a sample would be a group of people who have responded and agreed to be selected from among many to participate in a survey. Sampling in research would, therefore, be the process used to choose representatives from among a population to be employed in a research exercise. To successfully do this, inferential statistics was used to enable the researcher to determine a population's features through discernment of the samples used.

Assumptions

A fundamental assumption going into the study was the fact that cyber systems are at risk because of increasing numbers of cyber-attacks, thus indicating the need for cyber users to be more aware of security while using the Internet. While this assumption can only be verified by comparing relationships between study variables, it is nonetheless important as it gives an opportunity to explore more and understand some of the gaps that are noticeable in literature.

Although survey data and literature may not be enough to cover all the existing deficiencies in the literature and also may not help raise awareness on the importance of Internet security, other avenues like cybersecurity training, education, and organizational policies might cover the missing gaps in the literature.

Scope and Delimitations Inferences

Although cyber-attacks affect every Internet user, studying it from a global perspective is impracticable as it would be too broad. The approach used in this study was to address the issue from a targeted population and then make extrapolations from the results. Although the hypothesis of the study was developed based on existing literature and theory, it will subsequently be tested (Wilson, 2010). This method gives the researcher the ability to reason from the particular to the general.

The scope and sample of this research were students in the Washington, DC, area. This scope helped in data management and analysis. Following a deductive methodology, a set of hypotheses were formulated, and those hypotheses were tested to determine if they should be rejected or not.

A major problem that the research intends to discuss is the reality of the changing nature of crime. Traditionally, the field of conflict analysis and resolution had primarily focused on addressing crimes committed by people through physical contact and interaction. This traditional approach has shifted with the advent of technology based crimes as criminals operate in the shadows of software (Coleman, P. T. (2011).

Such a change presents a challenge that conflict resolution and risk management practitioners must confront by adjusting the way conflicts are traditionally analyzed and resolved (Coleman, P. T. (2011). The focus of the study is to raise awareness of the changing and challenging nature of cybercrime, and prompt researchers to create value by making the necessary adjustments needed to meet the evolving realities of the time. Actions of terrorist groups like ISIS who use social media to spread their terrorist ideology is proof of this challenge.

Limitations in the Study

Although Internet usability is valuable to people all over the world, its security problems create insurmountable risk to users who in some cases are seen to be "the weakest link in the cybersecurity chain" (Sasse & Flechais, 2005, p. 13). The focus of this study is to determine if cyber users' attitudes have any relationship with the occurrence of cybercrime. This knowledge will help educate cyber users on best practices that are needed to promote data availability, integrity, and confidentiality. The methodology used for the study only demonstrates the relationship that exists between the variables of the study and does not determine whether the occurrence of one variable causes the other. While this might seem to limit, it lays the groundwork for future fact-finding studies.

Although engineers and cyber users are working tirelessly to meet the challenges presented by continuous technological innovation, such efforts fall short as they focus more on technical fixes, thus limiting the ability to address the cybercrime problem which, has many components. While it is important to address technical challenges, users' attitudes and operational policies should be examined and improved because people are the ones using the Internet. (Mitchell & Nault, 2003). Constant technological innovation and development also makes it challenging to adequately address the cybercrime problem thus posing a challenge going into the research, for even if users improve their attitude towards security, constant technological innovation will still present a challenge

This notwithstanding, the resolution in this study is for IT risk management to be approached from a broader perspective and continually make adjustments to meet the challenges presented. Note should also be taken of the fact that shifting focus is not the only problem considering that there are growing security requirements, ever-rising costs,

efficient allocation of resources, and patronization of safety investments (Acquisti, Friedman, & Telang, 2006).

From the above points, an effective information security risk management framework must be eclectic in the sense that users and organizations must share best practices with each other and at the same time deploy the best and latest technological tools (Bostromand & Heinen, 1977). The challenge going into this research is then how eclectic could one go to address all the potential problems effectively. Scholars, managers, and policymakers should engage in a solution based approach to this issue by analyzing relevant theories and statistical data from different disciplines and then developing theory informed by best practices.

Though data gathered from literature and survey responses played a significant role in how conclusions were formulated in this research, such data was still limited as technological innovation is ongoing, thus presenting new challenges that take a long time to be understood and addressed. The fact is that producing new hardware and anti-virus software is critical in protecting data, but users should regularly reallocate resources and approach the issue of cybersecurity risk management from both the technological and the human perspective to be effective (Mitchell & Nault, 2003).

One possibility going into the research was that of porosity. Although analysis of variables would form an integral part of the methodology, it was possible that during such relationship inquiry, gaps in literature could appear. This notwithstanding, this possibility was contained by the use of controlled variables in covering the gaps and expatiating discourse on the relationship that exists between the variables.

Significance of the Study

The focused on understanding the relationship that exists between attitudes of cyber utilization and the security of the Internet so as to expand knowledge needed to address cyber risk and conflict when they do appear. In this world of information technology, crime is taking various forms and researchers must continually adjust their approach to meet the challenges that are presented (Coleman, P. T. (2011). Conflict resolution and crisis management practitioners cannot continue to do business as usual and expect to address current day problems adequately.

Cyber-attacks have revealed another phase of criminology, and both researchers and practitioners must adjust theory development methodologies and tactics to meet the changing times (Coleman, P. T. (2011). Survey data analysis would produce the findings of the study thus opening new avenues of orienting cybersecurity research.

Survey results would highlight the shifting realities existent in cybersecurity and indicate areas that need repair. Cybersecurity training would be one great way of improving security in IT. These shifting dynamics would help policy makers create legislation that would govern cyber usage in ways that limit risk and cyber warfare.

These findings will also open links of partnership between the departments of conflict resolution, engineering, and computer science on how to approach cybercrime. The methodology used in the study shows the relationships existent between the variables thus laying the groundwork for further research aimed at addressing the cyber threat.

Conclusion

In this chapter, literature on cyber usability was briefly reviewed and the justification for the dissertation was introduced. The research questions were also

presented as well as the scope, objectives, limitations, and relevance of the study. Finally, the chapter also looked at conceptual frameworks of the study, as well as explained and justified the variables chosen for the study.

Chapter 2: Review of Literature

Introduction and Restatement of the Research Problem

The advent of information technology systems like the Internet and others have generated a communications revolution in today's society. Through the Internet, people from all corners of the world get connected and carry out daily business easily (Howard, 1997; Sterling, 1992). Thanks to the Internet ideas about education, business, healthcare, finance, and other important issues of life are circulated to a wider audience quickly and securely (Cairncross, 1997; Dizard, 1997; Etzioni, 1997; Fishkin, 1992; Moore, 1987; Schwartz, 1996; Sproull & Kiesler, 1992).

Although the Internet is very beneficial to all people, its use has produced new forms of criminal actions, especially those posed by hackers who are ready to break into networks and steal data for their personal gain (Goodell, 1996; Littman, 1995).

Though hackers are ready and willing to break into systems and steal data, cyber users' attitudes towards security sometimes aid the work of hackers. Such activity explains why understanding the relationship that cyber users' attitudes have towards the security of the Internet is essential to this study. To create a more manageable scope for the research, the study sampled students in the Washington, DC, metro area.

The word hacking connotes the act of illegally breaking into computer networks and the Internet to steal data for personal gain, and those who personally commit themselves to these kinds of illegal activities are called hackers (Howard, 1997; Hutchison, 1997; Rasch, 1996; Stoll, 1985; Taylor, 1998).

Hacker as a term has assumed many connotations over time. It originally had a positive association that described outstanding programmers in the computer science field

(Chandler, 1996). As the years went by, and smart developers continued to research and develop software used to crack code and perform penetration testing and ethical hacking, its meaning gradually took a negative meaning and referred only to individuals who engage successfully or unsuccessfully in unauthorized penetration of firewalls with malicious code for their own unlawful and personal gains (Howard, 1997).

Because hacking arose as a new form of criminality with the invention of the Internet, cyber users and researchers are still trying with difficulty to develop ways to minimize its devastating effects (Hafner & Markoff, 1995; Hutchison, 1997), and the problem emerges from the constant development of IT and changes in methods and techniques used by hackers. For this reason, information security literature is still scanty and unable to adequately address the different components of cybercrime, as well as the behavioral traits of those who perpetrate it (Karnow, 1994).

The existence of cyber-attacks perpetrated by hackers has imposed the creation of information assurance or cybersecurity as a new field of study. This area of study sprung from computer sciences a few decades ago, thus explaining why researchers are vigorously compiling an extensive repertoire of literature that could explain the cyber-threat problem (Hutchison, 1997). For this reason, theories are borrowed and expanded upon from other disciplines such as psychology, criminology, sociology, law, computer science, IT management, conflict management and others to explain cybercrime.

This eclectic methodology of literature development is wise, considering that the cybersecurity field is broad and building active cyber defense systems must include the technological and the human components of IT. Through this method of theory development, some new themes are identified and analyzed. Some of these themes are

proactive security culture, internal controls assessment, security policy implementation, individual values and beliefs, and security training.

It is important to indicate that the broad scope of the field of cybersecurity has unavoidably compelled cybersecurity researchers to approach investigating cybersecurity issues from specific and isolated angles that help answer their research focus. Obtainable literature suggests that this approach has been somewhat biased as more resources are directed towards the technical and technological areas of the subject (Bostromand & Heinen, 1977).

Although expanding technical IT knowledge is important, focusing solely on technical expertise is problematic as it excludes that all important human factor input. An effective strategy to address the cyber-threat problem should not just concentrate on the technical but also include the human and the non-technical components of IT since technology is used by people.

While more has been done on the technological side, there is increasing literature that focuses on incorporating the human factor components of IT. The problem is that such literature primarily views users as isolated individuals in their approach to addressing cyber threat. Although it is encouraging to see an increase in the human factor research in cybersecurity, focusing only on cyber users individually is also limiting since individual actions on the Internet affect millions of other users. Therefore, engaging in a technical but also a psychosocial approach to addressing the cyber-threat problem is a better approach (Mitchell & Nault, 2003).

Theories that lie in the intersection of social psychology and technology gives a much better comprehensive analysis of what might be going on with cybercrime. The

field of social psychology offers complementary views with a rich body of literature explaining how an individual's actions strongly affect or are strongly affected by others. Social norms and many other social variables influence people's attitudes on how to approach risk. Normative group influences inspire humans to act a certain way, and these social standards affect human behavior in many ways.

Nolan, Schultz, Cialdini, Goldstein, and Griskevicius (2008) support this stance by asserting that in a situation where people desire to conserve power, telling people in a particular settlement that their neighbors were saving power increased the conservation of energy more than using non-social intervention strategies like telling them that preserving power was good for the environment and would save them some money. Taking the hotel industry example, Goldstein, Cialdini, and Griskevicius (2008) underlined that by only telling hotel guests that most visitors are opting to reuse their towels increases the rate of hotel room towel reuse by a significant percent.

The above two examples only explain the power of social intervention strategies in addressing issues. In this research, embarking on a psychosocial approach to dealing with the cybercrime problem would be helpful considering the vast nature of cybersecurity.

An eclectic and all-encompassing cyber-threat approach is the method employed in this research to explain the relationship that exists between cyber users' attitudes towards security and the occurrence of cybercrime. Analyzing users' experiences on current cybersecurity attitudes through surveys is relevant to this research as participants responses to the questions on the research questionnaire would produce results that would

help design enduring lessons and propose all-encompassing intervention strategies urgently needed to fight cybercrime.

Synopsis of Themes and Theories

Information security research is a critical academic exercise because it helps develop the tools, theories, and principles that ensure data availability, integrity, and confidentiality. From existing literature, critical topics concerning information security are developed and analyzed. Some of these are questions that deal with information security effectiveness (Kankanhalli, Teo, Tan, & Wei, 2003; Straub, 1990; Woon & Kankanhalli 2003), information security planning and risk management (Soo Hoo, 2000; Straub, 1990; Straub & Welke, 1998), the fiscal value of information security (Cavusoglu, Mishra, & Raghunathan, 2004a, 2004b), and finally the design, development, and best practices needed in the information security industry (Doherty & Fulford, 2006; Siponen & Iivari, 2006).

While these studies play a great and valuable role in educating users on the importance of cybersecurity, more research is needed to adequately meet the daily and evolving challenges posed by cyber-attacks (Siponen & Willison, 2007). Threats to information systems mostly not only come from hackers and organized criminals but also from authorized inside users who for some reason fail to maintain security while surfing the Internet. Studying and understanding the relationship that exists between cyber user's attitudes towards the security of the Internet is not only an important function of information security but also a function of the users that operate these systems.

Since the focus of this research is to look at the relationship that exists between users' actions and the occurrence of cybercrime, literature development focuses on

looking at what role cyber usability has on the phenomenon of cybercrime from both the user and the hacker's viewpoint. Approaching research and theories from this angle broadens understanding and develops an eclectic body of knowledge on the subject.

To develop an effective information security body of knowledge, both the technological and the human factors of cybersecurity must be considered since computers by their physical nature represent the functioning of a technical product which, must be operated by the end-users and affected by their attitudes, and biases (Mitchell & Nault, 2003).

Cyber users could also be hackers whose sole purpose is to cause harm by breaching security and stealing data or committing cybercrime. System users could also be authorized users who, according to literature, constitute what is called the insider factor threat or the authorized user threat or employees who are approved to use a particular system (Neumann, 1999).

An emerging research stream on the human attitude perspective of information security focuses on end-user (insider) approaches and attempts to identify the factors that aid or destroy information security compliance. Current literature recognizes that insiders, a term that refers to users who are authorized to use a particular system (Neumann, 1999), may pose a challenge to an organization's network because their ignorance, mistakes, and deliberate acts can jeopardize information security (Durgin 2007; Lee & Lee, 2002; Lee, Lee, & Yoo, 2004).

Recent survey reports on the subject support the argument, as well as an FBI survey which, shows that 64 percent of survey respondents indicated that some of the

losses related to cybersecurity they have incurred are due to the actions of insiders (Gordon, Loeb, Lucyshyn, & Richardson, 2006).

Cyber users' attitudes are, therefore, a major player in shaping cybersecurity culture for business environments. Even though users are considered the weakest link in the security chain, literature also recognizes that users can help safeguard information and technological resources if they pay attention to safety and perform beneficial acts. To encourage and enable effective security on the Internet, individuals and organizations often develop security policies that guide operation and enable cyber protection. Unfortunately, such guidelines do not automatically secure networks as system authorized users do not necessarily comply (Stanton, Stam, Mastrangelo, & Jolton, 2005). The challenge, therefore, is to identify what determines users' compliance with security policies and expand the development of theory and literature to include those aspects.

Emergent Themes from Literature

When one carefully examines existing research on cyber threats, reoccurring themes are identified. These topics, though not exhaustive in themselves, reoccur because they touch on areas that need to be developed to address the cybercrime problem effectively. These themes create a solution-seeking mind frame and identify areas that need to be tackled to address cyber threat issues. These topics are persuasive proactive security culture, internal control assessment, security policy implementation, individual values and beliefs, and security training. An analysis of these subjects indicates their role in clarifying the type of relationship that exists between cyber user's attitudes towards the security of Internet, and also creates room for further inquiry to address the issue.

Proactive security culture. Information security literature identifies the development of a dynamic security culture as an important aspect of security governance. By implementing a proactive security culture in a cyber environment, data integrity, data availability, and data confidentiality are maintained, thus building business confidence, trust, and stability as all stakeholders are assured that the data they are using are not contaminated (Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006; Thomson & von Solms, 2005; Vroom & von Solms, 2004).

Internal control assessment. From information security literature it is clear that internal control assessment is encouraged as it helps maintain effective security governance (Warkentin & Johnston, 2006; Whitman, 2003). In business or organizational environments, internal controls such as good practices, procedures, policies, and responsibility structures help ensure the efficient management of risk for the protection of data assets (Dhillon, 2001).

Internal controls are necessary for an organizational setting because they help monitor change control and keep the system secure for audit purposes. They are put in place by management to monitor all the aspects of the system such as password protection, access control monitoring, and much more (Flowerday, & von Solms, 2005; Posthumus & von Solms, 2004; Rezmierski, Seese, & St. Clair, 2002). Internal control practices are also encouraged within private networks as they give the user the mandate to feel responsible for securing their network.

Security policy implementation. Security policy is what guides safe operation in an environment (Ward & Smith, 2002). Clear and concise security policies are important as they prevent unnecessary changes that might affect the environment negatively

(Campbell, Al-Muhtadi, Naldurg, Sampemane, & Mickunas, 2003). When created, these policies must be clearly communicated to users, monitored periodically, and updated as necessary. Users' responsibility and accountability in maintaining security policies are crucial to their effectiveness since unimplemented policies are useless.

Individual values and beliefs. Adequate security for an environment is only attained if users cooperate with the security configurations and policies. This cooperation is driven by users' values and beliefs (Magklaras & Furnell, 2005; McHugh & Deek, 2005). When security configurations and policies have been put in place and tested to be successful, normative control is what keeps the environment continually secured as users go about their business (Adams & Sasse, 1999; Schultz, 2002).

Normative controls here mean the continuous assessment of users' values, beliefs, and attitudes as far as security is concerned (Stanton et al., 2005). These normative controls could be done by management in organizational situations or by individual users in private network situations.

Security training. The importance of training in learning cannot be overemphasized for it is in training that people learn and get acquainted with new things. Security training is, therefore, important as it is what teaches users, not just about the importance of cybersecurity but how to enable and maintain security while on the Internet. Training eradicates ignorance which, is disastrous to any secure environment (Bottom, 2000; Orgill, Romney, Bailey, & Orgill, 2004; Whitman, 2003).

Security training is mentioned by most cybersecurity researchers as an important prerequisite for security governance in any environment. It not only helps better utilize the overall security infrastructure, but it also leads to better management of the internal

security controls and policies that are put in place (Adams & Sasse, 1991; Segev, Porra, & Roldan, 1998). Therefore, continuous security training is encouraged as it helps build a security culture which, is needed for the smooth functioning of operations.

The above themes are important pointers to areas that need particular attention in an attempt to address the cybersecurity problem. In order to make progress with this quest to understand the type of relationship that exists between users' attitudes and cybersecurity, and in doing so also demonstrate how cyber users can become better stewards of security, some of the theoretical frameworks that have been used to examine human attitudes in some disciplines are identified and later in the chapter examined to see their relevance in analyzing the research problem.

Although no one theory can adequately explain all the components related to the cybersecurity problem, some of the ones examined below have previously been successfully used by researchers to properly explain what determines users' attitudes towards security while on the Internet and what drives users to follow or not follow security policies (Herath & Rao, 2009). These theories and models are the social learning theory, the general deterrence and rational choice theories, the technology acceptance model, and the socio-technical systems theory.

Preview of Major Sections of this Chapter

In this section, the research problem was restated, and literature relevant to the study was reviewed. This was done by analyzing theories and themes that have direct relevance in explaining the type of relationship that exists between the study variables. The literature search strategies used in the study were also discussed, and the theoretical

foundations of each theory used were explained. Finally, the literature related to key variables was reviewed.

Literature Search Strategy Used in the Study

Information sharing and research is an important but sometimes complex and challenging undertaking in academia, which, involves not only reading and citing relevant material from primary and secondary sources but most importantly having the skill to maneuver through library databases and search engines to locate the right information for the topic under consideration. This dissertation project has not been different.

The main source of literature came from primary and secondary sources located in the Nova Southeastern University Library and other libraries around the Washington, DC area. Because the study centered on examining the type of relationship that exists between attitudes toward Internet use and security among university students in the DC metro area, the literature search strategy was to work with the staff of the aforementioned school library and query their databases with one or more suggested keywords like computer security, IT systems use, hackers, hacking, information security, cyber threat, Internet security, cybercrime, cybersecurity, attitude of Internet users, and much more. The material was also obtained from journals in the field as well as Google Scholar.

Because an increase in cyber threat and cybercrime in the past few decades necessitated the creation of cybersecurity and information assurance as an academic field of study, most of its literature concentrates on the past few decades especially the 90s. As a result, the scope of the research was narrowed to the last ten years and in critical cases stretching to bring clarity where necessary.

The focus on this time frame, as well as the slight stretch, is justified by the fact that from the 1990s, the Internet expanded from the military, academic, and research institutions, government, and big businesses to individual households. This expansion, coupled with the advent of the war on terrorism, saw an increase in hacking activity and cyber threat, thus prompting researchers to increasingly publish on the subject and in doing so also borrowing from traditional psychosocial theories to explain human attitude towards Internet usability.

This explains why some of the analyses were informed by traditional theories that intersect social psychology, criminology, and information technology. In some parts of the study material such as articles would extend the timeframe. Such cases are justified by the fact that those articles were found to be very informative and relevant in explaining and analyzing the concept to aid understanding and clarity, and also because although some of them were published more than a decade ago, they have been reviewed and edited to be relevant in analyzing recent happenings.

An example of such a case would be the theory of planned behavior (Ajzen, 1991), which, explains behaviors and their relationships with crime, as well as the space transition theory which, explains and predicts actions of criminals and analyzed behavioral patterns of the offenses committed in cyberspace. Although these and others might extend the scope of literature, they are very relevant and necessary in explaining the issue under consideration in this research, thus justifying their use.

It is important to highlight the fact that cyber-attacks do not happen magically but rather as a result of some form of human activity on the computer. Consequently, the

human factor must be taken into consideration. This then makes it impossible to analyze and truly understand cyber-attacks using technology alone.

Therefore, to examine cybersecurity, one most include theories from other fields such as psychology, sociology, law, criminology, management, and others to explain a phenomenon like cybercrime because it is caused by people who use the computer for the wrong reason. That explains why using an all-embracing method to describe cybercrime is adequate and involves borrowing from fields that existed long before the computer was invented.

Theories and Their Applications to Security

Review of literature has always been an important part of research, and it is critical as it gives researchers the opportunity to form an in-depth evaluation of existing literature in the area under consideration to develop theory and models that help explain the research question. According to Kerlinger (1979), a theory is "a set of interrelated variables, definitions, and propositions that present a systematic view of phenomena by specifying relations among variables, with the purpose of explaining natural phenomena" (p. 64). Creswell's (2003) explanation of theory is similar. Theories are relevant to every field of study as they help explain the characteristics and behaviors of certain phenomena and also help researchers develop models and hypotheses used to test the validity of their propositions (Pidd, 2003).

In this section, primary and secondary sources, scholarly articles, and other sources like dissertations and conference proceedings that are relevant to the topic of research are reviewed. In doing so, a description of each relevant theory presented as well as a critical evaluation of their significance to the research.

Also, the contributions of previous scholars on the topic are assessed, and by doing so, relevant information is identified, existing knowledge is outlined, and any gaps in the research are identified, thus giving the opportunity to make criticisms necessary in theory development.

Social Learning Theory and Cybersecurity

Ronald Akers' (2000) social learning theory is one of the major theories that helps explain deviant behavior and crime. According to Akers, deviant behavior and crime occur because people learn excess of attitudes and behaviors that favor breaking the law. Central to the theory is the concept of group interaction and learning which, acts as an unnoticeable influence to one's behavior. The whole idea of attributing deviant behavior and crime to social learning is not unique to Akers. Other theorists had postulated this idea to support their arguments as Akers himself contends:

> Social learning theory added concepts used in behavior learning theory, differential reinforcement, whereby "operant behavior" (the voluntary actions of the individual) is conditioned or shaped by rewards and punishments. They also contain classical or "respondent" conditioning (the conditioning of involuntary reflex behavior); discriminative stimuli (the environmental and internal stimuli that provide cues for behavior), and schedule of reinforcements (the rate and ratio) in which, rewards and punishments follow behavior responses. (Akers, 2000, p. 75)

Fundamental to Akers' social learning theory is Edwin Sutherland's (1947) Differential Association Theory which, argues that deviant behavior is learned through modeling or imitation and reinforcement from familiar groups such as family and friends.

The whole emphasis of relationship is central to Sutherland's theory because, according to him, when people get used to others through interaction, intimate bonds are created which, lead to an influence of behavior. For example, if a person joins a group of individuals who focus on hacking, that person begins to learn the techniques of hacking, thus eventually transforming into a hacker. This is the same for an employee who gradually develops an attitude of indifference towards security by joining a company whose employees violate security by failing to protect their passwords and opening unrecognized links (Akers, 2000). According to Akers then, abnormal behavior and delinquency are learned because of an excess of definitions favorable to violation of laws (Akers, 2000).

Akers' social learning theory, just like Sutherlands' differential association theory examines factors that aid criminal behavior from the same lens (Blackburn, 1993; Gattiker & Kelly, 1977; Hollin, 1989). Most sociologists argue that the differential association theory provides the best conventional formulation and explanation of criminality because the theory asserts that people learn deviant behavior the same way they learn other forms of behavior with interaction and communication playing an integral role.

According to the differential association, when people interact with criminals they gradually start to learn the underlying motives, drives, rationalizations, and attitudes that nurture criminalization (Sutherland, 1947).

In Sutherland's words, the differential association theory leads modern society to be inherently built by conflicting ideas of what is considered normal behavior, and these conflicting layers of action contradict each other and generate conflict or crime

(Blackburn, 1993; Feldman, 1993; Gattiker & Kelly, 1997; Hollin, 1989; Sutherland, 1947). At the middle of these conflicting and contradicting forces lays communication which, comes in the form of peer pressure. This peer pressure influences behavior and pushes an individual to commit a crime, especially if their peers express ideas that are favorable or sympathetic to crime.

It is important to indicate that like all theories, the social learning theory and all theories that propagate learning and interaction as determinants of behavior have their limitations. In explaining and associating the cause of deviant behavior to interaction and learning from others, they fail to account for the origins of criminal definitions. This is a critical oversight because it fails to give people clues of what they are getting into right before they choose to join a group only to discover the bad influence the group has had on them later.

Additionally, although peer pressure, interaction, and influence play important roles in the social learning theory argument, all forms of criminal acts cannot be associated with peer pressure alone as many motivating factors exist. Cybercrime in many ways is a unique form of criminal behavior that sometimes entails intense technical configurations and operations that necessitate more than just peer pressure, communication, and interaction to carry out. Some of the cyber-attacks are highly sophisticated and require special schooling in engineering, computer sciences, networking, and information technology to build the capability to carry them on. That explains why governments and military establishments now have cyber defense departments that focus on developing the capacity to perform penetration testing, ethical

hacking drills, and cyber defense or cyber offense engineering training that help protect their systems and also go on the offensive if attacked.

It is important to indicate that though the social learning theory explains criminal behavior to a certain extent, it could equally be used to prevent deviant behavior if interpreted in the opposite. This argument is supported by Siegel (2006) when he contends:

> If people can become criminals by learning definitions and attitudes towards criminality, then they can "unlearn" them by being exposed to descriptions towards typical behaviors. It is common today for residential and non-residential programs to offer treatment programs that teach offenders about the harmfulness of drugs, the destructive nature of delinquent behavior, and the importance of staying in school. (p. 242).

The criminal justice system can also use the principles of social learning to set up diversion programs that help remove criminals out of the channels of the criminal justice system into rehabilitation programs that embrace learning through interaction to teach offenders to change by pairing them with good mentors (Siegel, 2006).

Embracing the social learning theory principles, a cyber awareness campaign could be developed that would reduce cyber risk by using the social learning theory principles to enable cyber users to identify and team up with recognizable peers who are knowledgeable in IT security practices and learn by imitating their safety practices.

General Deterrence and Rational Choice Theories of Cybersecurity

The General Deterrence Theory is borrowed from criminology to explain deterrent actions of cyber criminals (Parker, 1998; Straub & Welke, 1998; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Deterrence theory implies a practice where individuals are deterred from engaging in a criminal behavior because of the legal sanctions or repercussions attached to it.

The general deterrence theory like the rational choice theory assumes that human action is driven by sound decisions that are informed by the probability of severe consequences (Gibbs, 1975). The rational calculation is that legal punishment disrupts the propensity to commit a crime, and in this case cybercrime.

Deterrence theory and rational choice theory influences each other as they both utilize practical principles to push for reasoned action. Since human beings are rational, they make a cost-benefit analysis before making decisions. Such an ends and means calculation helps people make choices that are driven by the maximization of each other's pleasures. In situations where deterrence is present, choice helps the individual think through the potential pain or punishment that could be levied if one violates policy (Parker, 1998). In a cyber breach situation, one would think of the penalty associated with the crime and make a cost and benefit analysis before deciding to avoid the act.

The fundamental principle that upholds the deterrence theory then is the swiftness, severity, and certainty of punishment associated with violating the law (Felson, 1994; Liska, 1987; Messner & Rosenfeld, 1994; Pfohl, 1994; Pfuhl & Henry, 1993; Siegel, 1992).

According to the general deterrence theory, deterrent actions are right either at the individual or organizational level as a restrictive measure for a crime. In corporate settings, deterrence helps limit or prevent employees from violating policy as they are afraid of the consequences that may be levied on them. If such deterrence relates to upholding security while on the web, users—for fear of the repercussions of a violation—would adhere and by so doing help keep the system secure.

Deterrence can also go a long way to affect not only the behavior of insiders in an organization but also the behavior of outside offenders who might be willing to commit a crime but get scared because of the punishment that awaits any violators if caught. Though one could argue that some people avoid committing a crime for fear of being punished, it is hard to prove as no one knows what could go on in someone's mind at the time they make the decision to hold back. Situations like the Edward Snowden's leak of classified information indicates that, despite the laws put in place to punish criminals, deterrence does not always prevent cybercrime although his unique situation should be considered as an exception.

Technology Acceptance Model and Cybersecurity

The Technology Acceptance Model (TAM) is an information systems theory that explains what motivates users to accept and use technology. According to this model, IT tools cannot deliver improved organizational effectiveness if users fail to embrace and use them effectively. The technology acceptance model was originally proposed by Davis in 1986 and has gained respect in academia because of its role in explaining what motivates people to use technology. Another reason this theory is recognized is that of its

role in predicting what drives people to embrace technology use (Legris, Ingham, & Collerette, 2003).

The technology acceptance model expands Ajzen and Fishbein's (1980) theory of reasoned action and asserts that an individual's acceptance or non-acceptance to use technology is determined by perceived usefulness and perceived ease of use of the technology in question (Davis, 1989). This understanding highlights the fact that for an individual to use technology, he or she must not only know how to operate the technological tool but also acknowledge the importance and usefulness of that piece of technology to serve the intended need. If one or both of these points are not there, the individual will not feel comfortable using the technology. The presence of the above two points creates confidence and ascertains data availability, confidentiality, and integrity especially when dealing with both personally identifiable and financial information.

In line with the technology acceptance model, Fishbein and Ajzen's theory of reasoned action asserts that one's intention to behave a certain way in a certain circumstance depends on one's attitude as well as his or her subjective norms. Subjective norms here denotes "the person's perception that most people who are important to him or her think he or she should or should not perform the behavior in question" (Fishbein & Azjen, 1975, p. 302). Subjective norm is an important determinant of intentioned behavior here because one could choose to perform a particular action although he or she knows that it is not favorable (Venkatesh & Davis, 2000).

To adequately explain what motivates an individual to use a particular piece of technology, four categories are discernible. These classes are the individual context, the system context, the social context, and the organizational context. The social context

focuses on social influences that enable one to accept or not accept to use technology. The corporate setting centers on what an organization can do to motivate its employees to embrace and use IT systems securely. Thong, Hong, and Tam (2002) believed in the impact of the organizational context and expanded it also to include system visibility and network accessibility as one of the factors that motivate users to accept and use technology securely within an organization.

According to the technology acceptance model, context plays a significant role in determining what action one would take since the difference in capacity of attitude versus subjective norm to forecast one's intent to behave a certain way depends on the context. For example, if one is in a situation where self-influence is stronger than perceived subjective norm, then attitude would predict behavior intent the most. At the same time, if one is in a position where the normative implication is the dominant determinant of behavior, then subjective norm would be the primary predictor of behavior intent. If a user is a novice in technology, the subjective standard will probably be the most important determinant of one's technology use behavior (Taylor & Todd, 1995).

Many studies indicate the use of the theory of reasoned action to predict people's behavioral intent to use technology (Bobbitt & Dabholkar, 2001; Davis, Bagozzi, & Warshaw, 1989; Sheppard, Hartwick, & Warshaw, 1998; Venkatesh, Morris, Davis, & Davis, 2003; Yoh, Damhorst, Sapp, & Laczniak, 2003). However, there is the problem of contradictory results related to the confounding relationship between subjective norm and attitude and the assumption that intention leads to action which, warrants the need for further research and inquiry, thus necessitating input from the technology acceptance model of Davis (1989).

Although the theory explains motivations and attitudes of behavior to use or not use technology safely, it fails to acknowledge the fact that ignorance also plays a big part in users' inability to securely use technology as can be seen in victims of social engineering attacks. The model also fails to indicate that cyber criminals or hackers do not care about motivation to use or not use technology but rather are focused on the benefit that their illegal activity will give to them. The theory also fails to indicate the greed factor as a motivation to criminal behavior on the Internet.

Another issue is that there is no absolute measure of ease of use or usefulness of a particular action, as well as the fact that user perceptions of these constructs may vary with time and experience for any given application. Despite these limitations, the theory expands cybersecurity usability arguments further by its ideas and could be used to propagate the importance of cybersecurity training since perceived ease of use is identified as one of the factors that could hinder a user from actually using technology.

Socio-Technical Systems Theory and Cybersecurity

The socio-technical systems theory was coined in 1960 by Fred Emery and Eric Trist. This method was invented because businesses at the middle of the 20th Century were not achieving high levels of productivity compared to the degree of investment flow in technological systems. To address this issue, an argument was made that organizations would make more if they are treated as socio-technical systems where the technical and the social systems work together to produce high productivity (Schneberger & Wade, 2008, as cited in Gupta & Sharman, 2008).

The socio-technical systems theory is a perfect approach that should be used to explain today's complex organizational operations. According to this theory,

organizations are composed of both social systems and technical systems which, though independent from each other, work together in an interactive fashion to produce the desired productive results needed in an organization. The social system component of the theory centers on the people and the programmatic processes while the technical system component focuses on the technical methods used to transform input into output (Bostromand & Heinen, 1977).

Emery and Trist's (1960) socio-technical systems theory are important in organizational frameworks because of the everlasting increase and dependence on technology for efficient business delivery. In order for cyber users and businesses to improve their security investments a holistic approach to security is needed which, optimizes and utilizes the intrinsic interrelatedness of the social and the technical components of business delivery for better productivity (Mitchell & Nault, 2003).

Effective cyber usage, therefore, requires that cyber users not only learn and use the technological tools that are necessary for efficient business delivery but also embrace a positive business ethic and protective attitude needed to defeat hackers and their social engineering tactics.

Fontes and Balioni's (2007) study, in an effort to promote secure and efficient IT system delivery, indicates the relevance of the socio-technical systems theory in information security by arguing that information security professionals should stop perceiving information security systems from a more technical perspective, and expand their perception to embrace the human and the social aspects so as to reap the benefits of secure and collaborative business delivery.

In the same light Chaula (2006) argues that to produce a balanced and secure business delivery process, organizations and users should invest in and utilize both the technical and the social aspects of systems delivery.

Von Bertalanffy's (1968) systems theory, which, was introduced in the 1940s, actually laid the foundation upon which, Emery and Trist's socio-technical systems theory could thrive. His system approach draws from the concept of an organism which, has many parts and works together to complete a task and also achieve a state of equilibrium (von Bertalanffy, 1968). According to von Bertalanffy, this system has a single objective and is mechanistically oriented and evaluated regarding mathematics, feedback, and technology.

Hammond (2010) not only expanded upon von Bertalanffy's system theory concept but related it to an organization by stating that all components of an organization just like a system must function properly together to accomplish the organization's business objective. This analogy of a system indicates that, for an organization to work properly in a way that minimizes security threats it is necessary for all its elements to function in a collaborative fashion.

Drawing inspiration from the socio-technical systems theory, cyber users should develop an affirmative affinity to learn and use technology in an efficient and secure way for the safety and efficient delivery of their business. This attitude helps cyber users to identify and dismantle social engineering tricks before they deployed.

While acknowledging the usefulness of the socio-technical systems theory as a near perfect model for efficient network usage and delivery, it, unfortunately, fails to recognize and discuss the presence and devastating impact of those whose only goal is to

access networks to steal and destroy data. This omission seems dangerous and naive for the simple reason that although system operations might work collaboratively, there are not automatically shielded from daily threats. Therefore, continuous monitoring techniques must be employed and new defense techniques incorporated to enable systems to operate as intended.

To conclude, it is important to indicate that the socio-technical systems theory just like any other theory has its advantages as well as disadvantages since no single approach can analyze all aspects of a subject.

Summary of Theories and Their Application to Security

The above theories explain the relationships that exist between cyber usability attitudes and security from unique perspectives. These perspectives shed light on a very broad subject and through their limitation also challenge researchers to continue exploring more ways of explaining cybersecurity. An integrative and all-inclusive construct for analyzing cybersecurity should be the goal rather than assume a narrowly construed cybersecurity pattern.

This integrative construct is important because it takes proper perspectives from a variety of theories to effectively explain security and at the same time puts each perspective in its appropriate context. With this approach, a researcher focusing on cybercrime would start his or her analysis by first acknowledging all the variables involved and then referencing existing theories to explain the situation at hand. This is important because some cybersecurity theories approach their analysis of information security by focusing on single factor approaches that significantly limit their ability to efficiently and more broadly analyze the incident at hand.

Literature Review Related to Key Variables and Concepts

Cybersecurity and cybercrime have parallelisms in this research not just because of the broad and interconnected nature of the research topic but also because of the subtleties that bind both concepts together. This explains why the 2010 UN General Assembly Cybersecurity Resolution focused on cybercrime as a fundamental challenge of cybersecurity (Resolution 64/211, 2009). Cybercrime is an area of cybersecurity.

Though used interchangeably, both terms are defined and analyzed to highlight their usage and relevance in the study. The focus here is to examine attitudes towards cyber utilization and security to understand the connections that bind them together to enable the occurrence of cybercrime. Cybersecurity is, therefore, a significant variable in the study which, is tested by usability attitudes of cyber users.

Information security. Information security is the bigger term when compared to cybercrime as it refers to the protection of information and the systems that store and transmit such information (Whitman & Mattord, 2011). The three key attributes of information security are confidentiality, integrity, and availability (Smith, 1989, as cited in Rhee et al., 2009).

Information security practice then refers to the information security risk management behavior which, incorporates the acceptance and implementation of information security technology and the development of a safety conscious attitude on cyber use. Accepting and implementing information security here refers to the use of information security software and its features such as anti-virus software, while the development of a safety care attitude refers to security compliance culture in using IT tools demonstrated through the use and implementation of things like strong passwords

and making frequent backups of data for replication and availability purposes (Rhee et al., 2009). A comprehensive definition would, therefore, be that:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against associated security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which, may include authenticity and non-repudiation; confidentiality. (ITU, 2016, para. 1)

The above definition of cybersecurity is relevant to this study as it paints a clear picture of the broad nature of the subject under consideration. This definition is significant because it shows a clear distinction between the initial understandings of the meaning of cybersecurity in the 1960s. In the 1960s when the first computers were invented, threats to cyber systems only came in the form of physical damage to the infrastructure or the hardware. Therefore, cybersecurity at that time focused on the protection of the physical and could only be partially relevant in this study. As time went on and computers became available to more people, threats to cyber systems increased and took different forms to include the software component, specifically data or

intellectual property, thus necessitating the expansion of the definition to suit the level and nature of the current threat.

Cybersecurity plays an indispensable but important role in the ongoing process of information technology development since information systems are worthless without an effective security mechanism for its hardware and software. Therefore, enhancing security by protecting critical infrastructure and data is essential to cybersecurity (Resolution 45, 2006).

Cyber threat deterrence should be an integral component of the whole cybersecurity and critical infrastructure protection strategy for private and government agencies. The overall cybersecurity strategy and agenda should first involve the development of technical protection systems and then second, the education of users to adequately and securely use IT resources (Schjolberg & Hubbard, 2005). This signals a relationship between the two concepts that needs to be explained.

To adequately address the ever-increasing technical, legal, institutional, and human challenges presented by the cybersecurity framework, a comprehensive and coherent strategy must be implemented taking cognizance of the role of different stakeholders involved (Schjolberg, 2008). That explains why the researcher summed up the theory analysis section by proposing an integrated cybersecurity theory framework.

The Phenomena and Definition of Cybercrime

The occurrence of cybercrime has been viewed as a far-reaching problem in the information security field, thus explaining why many cybersecurity theorists have written extensively about the cybercrime problem (Burstein, 2003). But what exactly is a cybercrime? The term cybercrime is sometimes used interchangeably with the term

computer crime, but both terms have some slight differences. Cybercrime has a narrower meaning than computer related crimes because it only involves a computer network. A computer-related crime is broader as it could include crimes that do not have a direct connection to the network but may just affect computer systems. A clearer distinction between the terms was established during the United Nations 10th Congress on the Prevention of Crime and the Treatment of Offenders (United Nations, 2000).

During that conference cybercrime narrowly understood as computer crime was defined to involve illegal activity committed electronically and targeting the security of computer networks and the data it contains (United Nations, 2000). Cybercrime understood broadly meant computer-related crimes included any illegal behavior committed related to a computer system and network. An example could be an illegal possession, offering or distribution of information using a computer system or network (Kumar, 2009; Nhan & Bachmann, 2011; Sieber, 2004).

A standard definition describes cybercrime as any activity in which, a computer or a network is used as a tool, a target, or a place to commit a crime. Though this definition is acceptable, it is broad and could be interpreted to include traditional crimes like murder if, for example, the perpetrator of the crime killed someone by hitting them with a computer keyboard, monitor, or desktop (Carter, 1995; Charney, 1994).

The different variations in definitions demonstrate the difficulties involved in giving a ‘one size fits all' definition to cybercrime as it has many different facets and describes a plethora of offenses that include traditional computer crimes and network crimes. Because of the differences involved in these crimes, it is hard to craft a single standard that would include all acts required.

Though a single definition is not what is important, getting a typology-related approach to the concept is better as it describes what type of cybercrime is under consideration. Since it has already been established that the term cybercrime covers a broad range of criminal conduct, the Convention on Cybercrime distinguishes four different types. These are offenses against data confidentiality, integrity, and availability; computer-related offenses; content related offenses; and copyright related offenses (Aldesco, 2002; Broadhurst, 2006; Gercke, 2006; Gercke, 2008; Jones, 2005). These typologies cover all forms of cybercrime except in situations of cyber terrorism which, have many other dimensions that are not considered in this research.

Threats to information systems have existed since the beginnings of the technology revolution in the 1960s. Since then various approaches to address the issue have been adopted, but none can claim to provide an absolute solution to the problem because technology is always changing as are the methods used by cybercriminals to breach security. To fully understand the depth of the problem of cybercrime, as well as appreciate the efforts made to address the constantly shifting parts of the problem, a background explanation of the issue is necessary.

The 1960s. As stated earlier, the first computer was used in the 1960s, and at that early stage offenses against computers concentrated on physical damage on the hardware and stored data (McLaughlin, 1978). Publicly known examples of such first crimes against computers were reported in Canada in 1969 caused by a fire in a university data center as a result of a riot from students (Kabay, 2008).

Around the same time discussions on the need to create central data storage facilities emerged in the United States, and during those discussions the possibilities of a

criminal attack on data centers and databases, as well as the resulting risk to privacy, was equally a call for concern (Miller, 1971; Sieber, 1977; Westin & Baker, 1973).

The 1970s. Almost a decade from the date the first computer was introduced, computer use continued to increase but mostly around research institutions, government laboratories, and the military. This greater use of computers in the 1970s saw a rise in cybercrime. At that time cybercrime also started shifting from the traditional physical crimes against computer hardware of the 1960s to new but sophisticated schemes.

Although damage to computer equipment was still a problem, incidents of illegal use of information systems and manipulation of electronic data started to emerge. The shift in business transactions from manual processes to computer operated mediums in the 1970s generated an increase in computer-related fraud, thus posing new forms of challenges to law enforcement. These happenings ignited legal debates in most countries, and the United States started to discuss the draft of a bill specifically focused on addressing the cybercrime problem (McLaughlin, 1978; Nycum, 1976; Schjolberg, 2004).

The 1980s. The 1980s were an exciting time in the United States as ‘pockets' of wealthy individuals started purchasing their computers, thus increasing potential cybercrime targets. The 1980s also saw increased interest in software products which, led to an increase in software crimes like piracy and patent related crimes. Mediums for criminal activity changed to include the ability to commit a crime without the need of physical presence or location. This new platform for criminal activity posed more challenges to law enforcement. Criminals also started developing and spreading malicious software leading to an increase in computer viruses. All these frightening

developments caused countries to start updating their rules to meet the requirements of a changing criminal atmosphere (Andrews, 1983; Bigelow, 1985; BloomBecker, 1981; Kabay, 2008; Schjolberg, 2004; Thackeray, 1985; Yee, 1984).

The 1990s. The 1990s stretch saw tremendous expansion in computer use. In the 1990s, the graphical user interface was introduced, and web application uses increased. This was the www.com age which, saw an increase in cyber threats due to the Internet. Legal data security issues arose as information released in one country could be assessed in another even if that information was illegal in that state (Sofaer & Goodman, 2001). Online services expanded, thus posing challenges to investigate crime due to data exchange speed.

The proliferation of the Internet in the 1990s also posed a moral problem as pornographic material could easily be accessed through the Internet instead of books, periodical, and tapes as was the case prior to that time. All these types of cybercrimes compelled the international community and the United Nations to develop legally binding ways to control and prevent computer and telecommunication related crimes through resolution 45/121 (United Nations, 1994).

The 21st Century. This century is the age where computers and the Internet exist in every corner of the globe and the development of broadband Internet makes access to the Internet easy to everyone. New technological appliances such as smartphones, iPads, and tablets now have connections to the Internet. This has caused new and complicated methods of committing cybercrime. Some of these are phishing attacks, botnet attacks, and all kinds of cloud computer related crimes. Automation emerged, and cybercriminals developed new and sophisticated ways to automate attacks on large networks. All these

developments have brought the cybercrime issue to the fore, and almost all businesses and governments are working hard to secure and protect their networks from attacks (ITU, 2012; Simon & Slay, 2006; Velasco San Martin, 2009; Wilson, 2007).

Attitudes Towards Cyber Utilization

The increase in threats against IT networks has encouraged researchers to study the relationship that exists between humans and technology adoption. This research has expanded literature by emphasizing that in order to actually reduce cyber risk within organizations, focus must be shifted towards addressing attitudes of computer users as much as addressing technical issues (CSO Staff, 2004; Pattinson & Anderson, 2007; Stanton et al., 2005; Trček et al., 2007; Vroom & von Solms, 2004). This shift aligns with Bruce Schneier's assertion that "the biggest security vulnerability is still the link between keyboard and chair" (CSO Staff, 2004, para. 5).

Although a perfect understanding of the interactions between humans and computers helps manage information risk, users and organizational managers are still sluggishly refocusing their resources on attitudinal aspects of IT as they try to reap the benefits obtained from positive computer user behavior. This slow shift is explained by the fact that not much research has been conducted to explain secure cyber usability. To justify the scarce cyber usability literature problem, Abraham in her attempt to study factors that affect users' cybersecurity behavior in organizations discovered a serious lack of literature as she could only cite one paper published by Thomson and von Solms, (1998) on the subject of users' IT security behavior (Abraham 2011).

Before proceeding to analyze cyber usability and security, it is important to understand the meaning of attitude since that would highlight the importance of a positive

attitude towards cybersecurity. Attitude can be described as "a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993, p. 1; Ferguson & Bargh, 2007). Another scholar describes attitude as "a learned predisposition to respond positively or negatively to a particular object, situation, institution, or person" (Aiken, 2000, as cited in Yushau, 2006).

An important point raised by both definitions is the fact that attitude can be used as a good predictor of human intention or behavior (Kutluca, 2011). Ajzen through his theory of planned behavior capitalizes on this by saying that users' propensity to behave a certain way are driven by their intentions which, in turn demonstrates their attitude towards that behavior (Ajzen, 1988, 1991). Attitude towards cyber utilization would act as a good predictor of how cyber users would approach secure cyber use.

Level of Education. An IT user's level of education has been discussed by theorists and cyber users as an important determinant of a cyber user's attitude towards security. The proponents of the cyber user's level of education argument contend that the higher the level of education of the cyber user, the greater the user's level of concern for Internet security (Bishop, 2000). The overarching principle behind this viewpoint is the belief that a cyber user's educational attainment helps increase their capacity to use the Internet securely and also develops the necessary awareness for maintaining or ensuring secure Internet use (Bishop, 2000; Jones, 2002). Supporting this theoretical perspective is also the argument advanced by proponents of the theory that most educated people are informed about the adverse effects of cybercrime and by being part of the workforce are well aware of the consequences of a cyber-attack on business (Jones, 2002).

Education, as mentioned here, is not training but rather the process of receiving or giving systematic knowledge in a school or university setting. The sense here is that the more advanced someone gets on the academic ladder, the better equipped they are to understanding and using the Internet securely. Though plausible, this assumption needs to be verified as counter arguments have been raised by some scholars who argue that factors other than level of education determine the user's concern for Internet security, for example, prior experience with Internet breach, past financial loss as a result of cyber breach, the user's gender, age and place of residence, the user's computer and Internet savviness, and the user's prior training on Internet security awareness (Czaja et al., 2006). This explains why it is necessary to test the education variable in the study.

Gender. The discussion on gender and its role in cybersecurity cannot be ignored because people of all genders use the Internet regularly. Central to this debate is the gender gap noticed not only in computer education but also in the IT profession. From literature, many scholars worry that there is a disproportionately small number of women in the information technology workforce than men. Some even argue that there is a long and disproportionate history between men and women when it comes to attitudes towards computer adoption, use, and security (Jackson, Ervin, Gardner, & Schmitt, 2001; McIlroy, Bunting, Tierney, & Gordon, 2001; Morahan-Martin, 1998; Schumacher & Morahan-Martin, 2001; Sherman et al., 2000; Weiser, 2000; Wolfradt, U., & Doll, J. 2001).

According to these scholars, women are less likely to use computers than men because they are more anxious than men and are victims of technophobia or less liable to adapt to the technology than men. Some even argue that males are more interested in

computers than females and consider computers important and unique (Levin & Gordon, 1989; Shashaani, 1997). Although these views seem biased and necessitate empirical testing, they nonetheless exist, thus justifying the rationale to include gender as an independent variable to be tested in the study.

Despite conflicting views inherent in literature about which, gender category is a better steward of cybersecurity, researchers stills consider gender to be a significant determinant of cybersecurity usability, and scholars noticeably have argued that boys are more interested in computers than girls and therefore enjoy working with them more (Collis, Kass, & Kieren, 1989; Fetler, 1985; Shashaani, 1993).

Chen supports this trend when he asserts that among high school students, males are more self-confident in their ability to use computers than females (Chen, 1986). This notion is backed by the fact that women in general and minority women, in particular, do not have a lot of successful female role models in IT to emulate (Collis et al., 1989).

This notwithstanding, research has also found that more men hold gender biased views about computer competency than women. In one study where students were participants, female students agreed with greater consistency than male students that people of all genders have equal abilities in computer competency (Collis et al., 1985; Levin & Gordon, 1989; Smith, 1986). Another researcher conducted a study that indicated that out of 378 first-year undergraduate student participants, little evidence was attained to justify that computer use was exclusively a male dominated affair (Francis, 1994).

The fact is that many factors explain gender differences when examining cybersecurity usability. So many studies highlight the lack of exposure factor when

explaining gender differences related to cybersecurity usability and argue that the more women are exposed to using computers frequently and in equal proportion to men, the more the gender cybersecurity usability gap will shrink (Arch & Commins, 1989; Chen, 1986; Shashaani, 1994). These views justify including the gender variable to the study.

Age. The discussion on the relationship that age has on cybersecurity usability cannot be ignored because people of all ages use the Internet regularly. According to a study conducted by Schwartz (1988), only 1% of people above 65 years identified owning and using personal computers. When looking at using other forms of technology like ATMs, some scholars argued that seniors are less likely than younger people to use them although this seems difficult to comprehend in this digital age (Czaja & Shark, 1998; Rogers, Cabrera, Walker, Gilbert, & Fisk, 1996; Zeithaml & Gilly, 1987).

In contrast, data from a survey piloted by the American Association of Retired Persons (AARP) indicated that majority of respondents of retirement age were prepared to use personal computers to conduct regular tasks like budgeting, accessing health or benefit information, and preparing taxes (Edwards & Engelhardt, 1989).

In another study that focused on email use of women aged 50 to 95 years old, a substantial majority of them indicated that they loved having computers in their homes and were willing to use computers securely to pay bills and communicate (Czaja, Guerrier, Nair, & Landauer, 1993; Czaja & Shark, 1998). These inconsistent views justify the necessity to test the relationship with empirical data obtained from research participants.

Residence Location. Including the residence location variables in the study lies at the heart of the "digital divide" debate and emanates from theories suggesting that people

who live in densely populated urban areas and connect to high-speed Internet have a higher probability of using the Internet securely than individuals who live in sparsely populated rural areas and may not have access to the Internet (Horrigan, 2010; Zickuhr, 2013).

Central to this debate is the idea that connectivity to high-speed broadband Internet is more guaranteed in urban areas than rural areas of the country. This disparity is caused not only by the lack of availability of broadband infrastructure but also the gap in broadband take-ups between demographic groups across socio-economic lines. The fact is that lots of citizens in the United States, especially those who live in rural areas, still suffer disparities in not only Internet use, but also slower connections, fewer choices, and quality of access (Horrigan, 2010; Zickuhr, 2013). Despite all of these arguments, the notion that better Internet access ascertains secure Internet use demands further elucidation, and that is why the results from survey data are critical to this study.

Conclusion

Review of literature on cyber users attitudes towards security in this chapter reveals the difficulties encountered in fully understanding and addressing the cybercrime problem, particularly because of the changing nature of technology, the multiple stakeholders involved and the intricate relationships that lie hidden in human attitude and secure technology adoption. All these issues highlight the importance of engaging in this study using a quantitative methodology that is informed by survey data. Literature also reveals that majority of users might fall victim to cybercrime not necessarily because they want to but mostly because of lack of adequate knowledge needed to use the Internet securely. Literature also shows that, although information technology is good and makes

life easy, people should use it with care as cybercriminals are ready and willing to violate security and steal data for their gain.

Lack of a theory that could explain all the intricate parts of cybersecurity usability as a whole also demonstrates not only the vastness of the concept but also its complicated nature. It is, therefore, important to engage in this study so as to understand the type of relationship that exists between cybersecurity and users' attitudes towards security. This knowledge is important as it would help cyber users benefit from the usefulness of IT while securing their data assets. The next chapter presents the methodological framework used in this study to investigate the relationship that exists between cybersecurity and users attitudes.

Chapter 3: Methodology

Introduction

The purpose of this section is to present the method used to administer the surveys and analyze field data collected through questionnaires to arrive at the research findings. The study explored attitudinal differences of university students towards Internet utilization and security in Washington, DC, in an attempt to understand the relationship that exists between cyber utilization and cybercrime. As observed in the literature review chapter, while the discourse of Internet security has gained prominence, there has not been much focus on the relationship that cyber utilization have with security.

The chapter also focuses on a rigorous scientific analysis of filed data with the overall goal of building from the results to improve Internet security and the protection of data confidentiality through improved user attitude. This is important as it will contribute substantially to either prevent or reduce the risk that occurs as a result of data loss (DL), financial loss (FL), and diminished reputation of an organization due to a cyber-attack. The field of risk, conflict, and crisis management is experiencing increasing challenges due to the constant changes in tactics, methods, and types of crimes committed by cyber criminals in the 21st Century. This is evident in the surge in cases of cybercrimes every year (Internet Crime Complaint Center, 2011).

The surge in cybercrime underscores the importance of improving attitudinal traits of Internet users towards security. But to do that the relationship must be understood. While such understanding is needed to enhance the development of secure software and hardware, it also helps software engineers and law enforcement officials to derive new and innovative ways of addressing cybercrime. As Chinua Achebe has

asserted in his book *Things Fall Apart*: “since men have learned to shoot without missing, he has learned to fly without perching” (1958, p. 22). Using such logic one could say that while law enforcement, conflict resolution practitioners, security engineers, and policy makers have learned to configure adequate cybersecurity mechanisms to protect their assets, hackers have also learned to breach security without notice. The challenge in this research then is to understand the relationships that cyber utilization have with security and determine best practices that could promote the secure use of the Internet.

Cyber-attacks are the unintended effects incurred by innocent cyber users. Such attacks are bad and should be prevented to promote security in IT. Developing an effective cybersecurity strategy that meets the 21st century IT challenges is something that cybersecurity professionals, crisis management practitioners, policy makers, law enforcement, and cyber users must confront. This is urgent because of the damage caused by cyber-attacks and the potential degenerating devastation such attacks could ignite on financial systems considering that almost every major financial institution in the world now depends on the Internet to conduct their business (Setia, V & Joglekar, 2013).

This chapter discusses the methodology used in the study. The study employed quantitative methodology and was designed as an association research aimed at understanding the relationship that exists between cyber utilization and cybercrime. To achieve this objective, surveys were used to collect data while Chi-square statistics was used for data analysis. This methodology was suitable for the study because it ensured an accurate elucidation of the relationships that exist between the research variables (Creswell, 1994; Reinard, 1998).

Survey research is relevant in exploratory studies, and as observed by some scholars, its goal is to respond to questions that are raised, to address issues that are seen, to measure needs and set goals, to determine whether or not specific objectives have been met, to create baselines against which, future assessments can be made, to analyze trends across time, and generally, to define what exists, in what amount, and in what context (Isaac & Michael, 1997).

The principles of association research used in the study help define the relationship between the research variables. This method helps with understanding how strong the relationship is and what type of relationship exists between the variables. The methodology of the study was chosen with three possible outcomes in mind: first, to realize a relationship, second, to indicate when a relationship does not exist, and finally, to realize when a relationship exist but is weak. Important to note is the fact that while an association study explains relationships that exist between two or more variables, it cannot show that one variable causes a change in the other (Isaac & Michael, 1997).

Therefore, a cause and effect quest is not the aim of this study as much as it is the nature of the relationships that exists between the research variables. This relationship helps explain the conditions that account for the occurrence or non-occurrence of cybercrime and also create space for further research that could explain emerging questions on the subject.

Among the many aspects of the research methodology presented in this chapter are the research design and rationale, the sampling procedures, the data collection procedures, the description of the data, the analysis and interpretation of the data, and the data manipulation procedures.

Central to this chapter is a detailed presentation of the various protocols and tools of the methodology used in the study. Some of the research tools discussed in this chapter are the questionnaire used in collecting the field data and the statistical test used to analyze the data. The chapter also describes the target population and the sample used in the study, as well as presents the justification and relevance of the utilization of the student population in the research. Finally, the chapter describes the procedures used to validate field data and administer incomplete data.

Research Design and Rationale

The study was designed as an exploratory study aimed at analyzing attitudes towards Internet utilization and security among students in the Washington, DC, area to understand the relationship that exists between cyber use and the occurrence of cybercrime. Since the research design is not only exploratory but also associational, surveys were used to obtain data and guide the researcher give an informed explanation of the relationship between the research variables. A 'survey' is a research methodology designed to collect data from a defined population, or a sample of that population by the use of a questionnaire or an interview as instruments (Robson, 1993).

Although many other techniques such as interviewing and observation could be used to collect data from a sample population in a survey, a questionnaire is widely used (Marsh, 1982) as was the case in this study.

Sample survey is an important method of data collection from selected individuals and has been used successfully by researchers in conducting and applying basic social science research methodologies (Rossi, Wright, & Anderson, 1983). Survey design, according to Levy and Lemeshow (1999), involves two steps. The first step is setting up a

sampling plan or the methodology that will be incorporated to identify samples from the population and second, determining the procedures that will be used to establish desired response rates (Salant & Dillman, 1994). These two steps will all be explained in the sampling section of the research.

This research was designed around the questionnaire which, was developed and posted on SuveyMonkey. SuveyMonkey is an online survey company that provides free and paid customizable services to researchers that include data collection, data analysis, sample selection, bias elimination, and data representation tools. The criteria for the selection of the participants included being a student and residing in the Washington, DC, metro area, using the Internet, and falling between the ages of 18 years and older.

Responses from participants were used to test the relationship that exists between the dependent and the independent variables of the study. Here are the research questions that were answered in the study: RQ1: Is there a relationship between the users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity? RQ2: Is there a relationship between the users considering themselves as IT savvy and their level of concern for cybersecurity? RQ3: Is there a relationship between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity? RQ4: Is there a relationship between amount of financial loss experienced due to cyber breach and level of concern for cybersecurity? RQ5: Is there a relationship between the Internet user's educational level and their level of concern for cybersecurity? RQ6: Is there a relationship between the Internet user's gender and their level of concern for cybersecurity? RQ7: Is there a relationship between the Internet user's age and their level of concern for cybersecurity? RQ8: Is there a relationship

between the Internet user's residence location and their level of concern for cybersecurity?

To test the above questions, the following researcher's hypotheses were examined. H1: There is a significant association between the users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity. H2: There is a significant association between the users considering themselves as IT savvy and their level of concern for cybersecurity. H3: There is a significant association between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity. H4: There is a significant association between the amount of financial loss incurred due to cyber breach and level of concern for cybersecurity. H5: There is a significant association between the educational level of the cyber user and their level of concern for cybersecurity. H6: There is a significant association between the gender of the cyber user and their level of concern for cybersecurity. H7: There is a significant association between the age of the cyber user and their level of concern for cybersecurity. H8: There is a significant association between the residence location of a cyber user and their level of concern for cybersecurity.

Using a questionnaire in research offers some unique advantages that are non-existent in other research methods like interviewing as they are not only easier to administer than conducting personal interviews but also ensure confidentiality (Leary, 1995). Questionnaires are also highly structured in collecting data as there ensure that all participants respond to the same questions which, might be problematic when conducting interviews (de Vaus, 1996) or employing other methods to collect data (McIntyre, 1999).

The findings of the study were drawn from a sample of 433 participants collected from among university students in the Washington, DC, area. The analysis of data was driven by the notion that there is a connection between Internet utilization and Internet security.

Data collection through a survey was, therefore, used not only because of the significant role it plays as a tool for collecting and analyzing information from selected samples but also because of the recognition it has established in social science research as a useful and vital tool for data collection (Rossi et al., 1983).

Survey was also used because it is known by many people in the United States, especially amongst the elite community. Many people in the United States have participated in marketing surveys that help business managers decipher consumer preferences or shopping patterns for effective management (Leary, 1995).

Many U.S. television viewers have also participated in the Nielson survey which, helps media executives quantify the number of audiences who watch particular programs for the purpose of establishing advertising rates. To carry out such Gallup polls, samples are taken from participants disaggregated by gender, ethnicity, education, and region in the country (Rossi et al., 1983).

Methodology

The methodology employed in the study is quantitative. Surveys were used with the aid of an electronically distributed questionnaire to collect data from the sample. In using sample surveys, the researcher systematically gathered information from a sample of students around the Washington, DC, area on users' attitudes towards cybersecurity.

Judgment sampling was used because the research required specific conditions for participation, and these specifications were clearly explained on the consent form at the beginning of the questionnaire. These specifications ensured that research participants agreed to the terms of the research and were within the criteria indicated. Data collected from the survey was then used in crosstabs to construct quantitative descriptors of the relationships that exist between cyber utilization and the security of the Internet (Groves et al., 2009).

The research population was deliberately chosen because of its accessibility and familiarity in using the Internet. University students use the Internet for a variety of transactions, some of which, are for research, education, communication, business, financial operations, and networking with the aid of social mediums such as Face book, MySpace, LinkedIn, WhatsApp, Twitter, and others. Before choosing the population, fundamental questions were raised and answered. Some of these were: Can the population be enumerated? Is the population literate? Are their language issues? Will the population cooperate? What are the geographic restrictions? (Trochim, 2006).

These questions and others played a key role in moving forward with the choice of the sample. Added to the above considerations, the researcher was comfortable moving forward with these criteria for participation because SuveyMonkey assured the researcher that it had more than enough registered members who met the research criteria from which, to pull.

The literacy rate of the population was equally considered. The questionnaires required respondents to be able to read, understand, and respond to the questions. Although the researcher quickly assumed that adults and most especially students could

read and understand English considering the expectant high literacy rate among students, some questions seemingly contained difficult or technical vocabulary. The pilot study helped the researcher address this problem by making the language less technological and easy to understand.

Also, by choosing to target a literate population and reviewing the language of the questionnaire after the pilot study, the researcher improved construct validity of the research by selecting the study participants carefully and making the questions accessible to all of them.

Geographic restriction issues are also legitimate to deal with before deciding what population to use for research. It is always important to know if the population of interest is dispersed over too broad a geographic range for the researcher to meet and interview participants. The geographic restriction was not an issue here because the researcher was using an electronically distributed questionnaire format which, did not necessitate physical presence or contact between the researcher and the participant. The researcher also did not need to interview the research participants as they just accessed and responded to the questionnaire on SuveyMonkey (Robson, 1993).

Sampling and Sampling Procedures

This study was designed to focus on examining attitudinal dynamics of cyber use and security in the Washington, DC, area. This focus regulated participants to a sample of 433 students in the DC area who were 18 and older. A sample of the study participants was obtained through a web-based survey and then exported to the SPSS statistical software for analysis since SPSS has been used successfully by many researchers to analyze data and produce results that are scientifically reliable and adequately explain the

question of the study (Witt, 1998). The SPSS software gives the ability to choose the statistical test needed to analyze the data.

Data collection is an important part of research as data helps create a better understanding of a theoretical framework (Bernard, 2002). Therefore, carefully choosing the technique used to collect data as well as the participants is critical to the success of a research project considering that no amount of analysis can make up for improperly collected data (Bernard et al., 1986).

Judgment sampling was used for data collection because it is a non-random technique that ensures that research participants are defined based on the objective of the research (Bernard 2002; Lewis & Shepard, 2006). Judgement sampling also made it easy to meet the number of participants needed for the study (Alexiades, 1996; Bernard, 2002) and ensured that data collected met the demographic stipulations of the research (McIntyre, 1999), thus making the research relevant to other students in the Washington, DC, metro area (Bell, 1996).

Irrespective of all the advantages presented by the sampling technique used in the study, the results of the pilot study played a key role in determining whether to proceed with the study or not. Data analysis from the pilot study with a small sample size of 50 participants indicated the need to increase sample size so as to avoid type I and type II errors. A type I error would occur when the researcher falsely rejects the null hypothesis, thus accepting a false relationship. A type II error would arise when the researcher erroneously accepts the null hypothesis, thus creating a false negative (Lieberman & Cunningham, 2009). To minimize such errors, a large sample size of 433 participants was determined to be adequate, and a confidence level of 95% with a 5% error chance and an

alpha level of 0.05 was adopted while employing Chi-square statistics to test the null hypothesis of the study (Lieberman & Cunningham, 2009).

Procedures for Recruitment, Participation, and Data Collection

The procedures for recruitment, participation, and data collection used in the research were ethical and met research standards. Research participation was voluntary, and participants were informed of the nature of the survey, their role, and potential benefit—which, was sole to increase knowledge—through a consent form which, was made available to participants at the top page of the questionnaire posted on the SuveyMonkey platform. This platform was adopted because it is the world's leading provider of web-based survey solutions, and is trusted by millions of, organizations, and individuals to gather the data they need to make informed decisions. SuveyMonkey is used by researchers worldwide to get the research responses they need in a very short period compared to other survey collection mediums (SuveyMonkey, 2015).

SuveyMonkey's management takes the responsibility to ensure participatory membership of diverse groups of people who are interested in sharing their opinions with researchers. SuveyMonkey membership is free, and the enrollment process ensures that new members complete a profile form with demographic questions on age, gender, region, and other targeting characteristics like job type, cell phone usage, and more. SuveyMonkey ensures that researchers get the responses they need by pulling from a diverse population of more than 30 million people who participate in their surveys (SuveyMonkey, 2015).

The SuveyMonkey web-based platform is widely recognized in the scientific community because of the high return rate and the high levels of neutrality experienced

with the surveys. Learning from the pilot study, the researcher limited the number of questions in the research instrument to an appropriate number, making sure that the questions asked were clear and had direct relevance to the objective of the study.

Part of the reason SuveyMonkey's online surveys are widely respected is also related to the fact that although contributing panelists come from a few countries namely, the United States, the United Kingdom, and Australia, researchers have the authority to choose the country and region from where to pull their respondents. SuveyMonkey panelists fall with the age of 13 and older, but researchers have the liberty to target respondents by age and in this case can limit the target population to 18 years and older depending on the demographic requirements of the research (SuveyMonkey, 2015).

To enlist with SuveyMonkey, the researcher made a professional subscription, selected the criteria of the study, paid the fee based on the criteria selected and uploaded the survey questionnaire on SuveyMonkey. SuveyMonkey engineers then forwarded the survey link to participants who met the researchers demographic and research criteria. SuveyMonkey was responsible for automatically balancing results according to census data for age and gender, and such balancing precision and granularity was adjusted and improved as responses increased in number. Once the researcher complied with SuveyMonkey policies and guidelines, the project was completed in just a few days as participants easily opened the survey link, responded to the inquiry, and returned their results via the SuveyMonkey website for the researcher to export to SPSS (SuveyMonkey, 2015).

The instrument of the research was the questionnaire developed by the researcher and improved through a pilot study that tested the clarity of the research questions. In

developing the survey, the researcher made sure leading questions were avoided, and the answer choices were mutually exclusive. To ensure that more in-depth information was provided by participants, the researcher ensured that the survey formulation consisted of closed-ended questions which, were based on the research objectives, questions, and hypothesis. The questions also followed a logical progression starting with demographic questions and proceeding to study specific issues which, progressed from simple themes to more complex problems aimed at progressively sustaining the interest of the respondents. All of these were tested by the pilot survey, and the final design was adjusted based on the results of the pilot test (Robson, 1993).

Pilot Survey Study

Before engaging in the study, the researcher examined the effectiveness of the questionnaire by selecting a smaller but similar group of 50 students to participate in a pilot survey to determine if the questions were yielding the kind of information needed to answer the research questions. To conduct the pilot study, the researcher explained his research topic to his church members, and 50 members who met the research criteria voluntarily accepted to participate. The researcher then provided the pilot questionnaire to them and asked that in responding to the questions they should indicate any areas that needed clarity for understanding (Robson, 1993). Responses and comments from the pilot study proved vital as they helped identify unforeseen contingencies and weaknesses that were addressed before the actual survey was conducted.

In particular, the pilot survey helped avoid misleading, inappropriate, or irrelevant questions that could have created inconsistencies and hinder the progress of the research

as those inconsistencies could have caused participants to skip some questions or out rightly refuse to participate (Fink & Kosekoff, 1985).

The pilot study did not only test the research instruments but also ensured that the survey instructions were comprehensible and the wordings were correct (Baker, 1994). The pilot survey instrument was the same questionnaire that was edited after the pilot and used in the research to evaluate cyber users' attitudes towards security.

Pilot study participants were instructed to indicate at the bottom of the pilot survey page what their thoughts were concerning the design of the questions. Most of the participants reported that the survey questions had few options and so they requested for more options on the questions. The researcher then edited those survey questions and provided categories of options to indicate users' level of concern for security while browsing the Internet (Baker, 1994).

Comments from the pilot survey were very helpful as they helped the researcher rephrase some questions to ease answering and in some cases gave the respondents more options, and that ended up helping the researcher better explain the operationalization and manipulation of the variables (Baker, 1994).

Updates made on the questionnaire as a result of comments from the pilot survey boosted the confidence of the researcher as he proceeded to the actual research survey with the sureness that questions were clear and easy to answer. The importance of the pilot study was just to assure the researcher that the questionnaire was clear and effective at generating the much-needed data through responses from participants (Robson, 1993).

Data Analysis and Interpretation Following the Chi-Square Correlation Analysis Model

The analysis and interpretation of the data was determined by the Chi-square statistics test results, and contingency tables were used to describe the data. Chi-square is a statistical test invented by Pearson to compare observed data with data that is expected to be obtained according to the hypothesis in question (Diener-West, 2008).

Chi-square statistic was used because it gave the researcher the ability to measure the occurrence of cyber-attacks by comparing the occurred or observed instances in each table cell to the instances which, were expected to occur or observed under the assumption of no association between the row and column classifications (Diener-West, 2008).

Chi-square statistic was also used here to test the hypothesis of association or no association between the variables by comparing the occurred or observed counts to the expected counts. By testing the strength of the relationship between the occurrence of a cyber-attack and other independent variables using Chi-square, Lambda, and Gamma, an informed theory was established from the results (Diener-West, 2008).

To choose Chi-square for data analysis, certain assumptions were made. The first assumption was that of independence of observations which, focused particularly on the fact that each participant's response was independent and told nothing about another participant's response. By assuming the independence of observation, the researcher was aware of the fact that that was only going to be achieved if the sampling of one observation did not affect the choice of the second observation (Diener-West, 2008).

The second assumption was that all categories would include all of the observations and avoid overlapping since the Chi-square test of association cannot be conducted when categories overlap or do not include all of the observations. The last assumption was the expectation of large sample size which, in this case met the premise as the study tested 433 cases (Diener-West, 2008).

Since the study questions sought to establish the degree of the relationship between the dependent and the independent variables, contingency tables were used to show patterns of relationships demonstrated by the variables in the cross-tabulation analysis. Cross-tabulation is a joint frequency distribution of cases based on two or more categorical variables. Such a display of allocation of cases by their values on two or more variables is called contingency table analysis (Diener-West, 2008).

Cross-tabulations were used to show the distribution of the observations of the independent variables across the categories of the cases of the dependent variables (Diener-West, 2008). In the contingency table, the dependent variables were placed in the columns of the tables while the independent variables appeared in the rows, and the examination of the frequencies of incidences of the occurrence of cyber-attacks across the categories of independent variables were used to analyze the crosstabs.

The use of crosstabs in the study helped determine the existence or nonexistence of a systematic relationship between the dependent and the independent variables. It also helped define the nature and strength of the relationship between the variables. Nature, as used in the context of the analysis, refers to the description of the relationship between the dependent and the independent variables. The relationship is described as either positive or negative (Diener-West, 2008). A positive correlation was determined to be

one in which, increase in attitudinal dynamics towards secured Internet use also led to increasing security and consequently, a reduction in incidents of cybercrimes. A negative relationship was determined to be one in which, decrease in attitudes towards secured Internet use led to increasing incidents of cybercrime.

Chi-square statistics was used to analyze the relationships between the variables. Before using Chi-square the following assumptions were taken into consideration:

1. The sample size assumption: Since Chi-square is used to determine the difference in the proportions of the observed and the expected frequencies, the researcher made sure that the sample size was large enough and equally representative of the characteristics of the sample (Diener-West, 2008).
2. The independence assumption: Considering that Chi-square cannot be used on related data, the researcher made sure that each variable was independent of all the others in the conceptual and the operational definition.

Considering that the research focused on explaining relationships among the study variables using data collected from a sample of 433 students in the Washington DC area, study results only reflected the views of the sample used. Taking into consideration this factor, the application of purposive sampling and Chi-square statistical tests such as the Gamma and Lambda were applied to explain statistical significance of the results.

The Chi-Square Formula Used in the Analysis of the Observed and Expected Frequencies

The Pearson Chi-square statistics was calculated as the sum of the squared difference between the observed (0) and the expected (e) frequencies or (the deviation, d), divided by the expected data into all possible categories or the observed minus the

expected, squared, and divided by the expected. The formula below was applied in the calculation of the Chi-square association (Diener-West, 2008).

$$X^2 = \sum \frac{(\text{Observed frequency} - \text{Expected frequency})^2}{\text{Expected frequency}}$$

Figure 1. Chi-square statistics formula.

The Chi-square value for the test as a whole is then calculated as the sum of the observed minus the expected, squared, and divided by the expected. The equation below demonstrates how Chi-square is calculated (Diener-West, 2008).

$$X^2 = \sum \frac{(\text{Observed frequencies} - \text{Expected frequencies})^2}{\text{Expected frequencies}}$$
$$= \sum \frac{(Fo - Fe)^2}{Fe}$$

Figure 2. Chi-square statistics formula expanded.

Justification for Using Chi-Square Statistics in the Research

Inferential statistics is important because it employs statistical methods that are designed to test hypotheses that capture relationships between variables. Although descriptive statistics also illustrates relationships between variables, inferential statistics techniques go a step further to demonstrate by the aid of a statistical test whether a relationship exists between research variables or not (Diener-West, 2008).

As already seen above, Chi-square statistics test was used in the study. This choice was determined by the categorical nature of the variables and the objective of the study which, aimed at showing the nature and statistical significance of the association that exists between the variables used (Diener-West, 2008).

Unit of Analysis

The unit of analysis for the study was students. Students were operationally defined and categorized to be anyone attending college or university in the DC area and fall within the age of 18 years and older. Categories of students were divided into three groups. Those within the age group of 18 and 30 were categorized as young age students, those 31 to 50 were classified as middle age students, and those 51 and older were classified as older age students.

Operationalization and Manipulation of Variables

Explanation and Manipulation of the Information Security Variable

As already stated in the literature, information security was conceptually defined in the study as the safeguard of information and the systems that store, and transmit such information (Whitman & Mattord, 2011). The three key attributes of information security considered when analyzing attitudes towards Internet security were data confidentiality, integrity, and availability (Rhee et al., 2009; Smith, 1989). Cybersecurity threats were defined to be security incidents that may compromise an IT asset, thus resulting in the occurrence of an undesirable consequence (Clarke, 2011; Summers, 1997).

The concept of information security practice was then used in the study to explain security risk management practices and security conscious attitudes of users. Computer crime which, was the aspect of security the study focused on was conceived in the research to be any illegal activity committed electronically and targeting the security of computer networks and the data it contains. In the broad sense of the word, cybercrime was used to denote any illegal behavior committed that has a relation to a computer system and network (Kumar, 2009; Sieber, 2004). Commonly described then, cybercrime

was seen to be any activity in which, a computer or a network is used as a tool, a target, or a place to commit a crime (Carter, 1995; Charney, 1994).

Field data obtained through a survey was presented in contingency tables. These tables displayed relationships between cyber utilization and security with the goal of determining if participants were concerned about secure cyber use or not. The security variable was presented in categories for easy comparison and interpretation. The security variable was operationalized into a likert scale of four categories. These were: very highly concerned, somewhat concerned, little concern, and not concerned. The question in the instrument that was used to test participant's level of concern for cybersecurity was question 8. Please rate your level of concern for cybersecurity?

The assumption underlining the study's theory was that users who have very high-level of concern for secured access to the Internet (Do Care Users) are most likely to develop attitudinal traits that favor secured Internet access while users with little or no concern (Don't Care Users) for Internet security are most likely to adopt attitudinal traits that disfavor secured Internet access. However, the underscoring factual reality of the above theoretical premise centered on whether or not users feel that security is important or have concern for security while using the Internet, as a cyber-attack is damaging to the integrity of any network and could cost users millions in losses.

Although the variables of the study were initially nominal variables, the researcher was able to manipulate some and transformed them to ordinal variables by grouping the responses into categories that reflected each user's level of concern for security. The category of "high" described very high concern for Internet security and the category of "somewhat" described medium concern for Internet security. The category

"little" expressed very little concern for Internet security, while the category "not concerned" explained no concern for Internet security.

The above categorization of the security variable facilitated the presentation and analysis of data in chapter four by equating the concern for security variable with each independent variable in contingency tables. This made it easy to identify security as the dependent variable in columns and the variables in rows as the independent variables.

Justification for Including the Information Security variable in the Analysis

Given the importance of this topic which, comes from the frequent devastation caused by cyber-attacks, it is important to empirically evaluate an understand security, considering the harm that cyber attackers inject on the economic and national infrastructure of nations (Schmidt, 2010). Cyber criminals continue to exploit vulnerable cyber users who have been identified as the "weakest link" in the chain of system security (Sasse & Flechais, 2005, p. 13). This loophole is real and most be closed for if Internet users remain indifferent to Internet security, more cyber-attacks will continue to occur (Sasse & Fleshais, 2005) thus justifying the importance of the security variable.

Explanation and Manipulation of the Attitudes Towards Internet Use Variable

Attitude was conceptually defined in the study as "a psychological tendency expressed by evaluating a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993, p. 1; Ferguson & Bargh, 2007). The attitudinal tendency to either favor or disfavor something is expressed in how people approach things as people's attitudes presupposes their action. Attitude towards Internet utilization as employed in the study explains the positive or negative outcomes that cyber use have on secure Internet

usability (Smith et al., 2000). Such attitudes could relate to cyber utilization in general or its specific functions like cybersecurity training or the type of transaction conducted.

Attitude towards Internet utilization also explains a cyber user's disposition either to favor or disfavor security and this disposition reflects the way the cyber user approach secure Internet utilization and its related functions. If a cyber user has a positive attitude towards cybersecurity training he or she would take training seriously thus enhancing secure cyber utilization. The attitudinal stance of a cyber user towards security determines their level of concern for security in IT (Smith et al., 2000).

Participant's attitude towards cybersecurity was captured with the question: Do you consider Internet security an important factor of your Internet use attitude? To answer the question, yes or no options were given to help participants indicate their attitude towards security. Participants who answered positively to this question indicated that they have a favorable attitude towards security which, is reflected in how highly concerned they would feel about security. Participants who answered negatively to the question indicated that they have an unfavorable attitude towards security which, is reflected in how less concerned they would feel about security.

Justification for Including Attitudes Towards Internet Use in the Analysis

Including attitudinal dynamics of Internet utilization in the analysis was important because the researcher believed that computers serve no purpose until there are used by a user and the tendency to use them securely is determined by the user's predisposition towards security. Based on this belief a cyber user's operational disposition towards the computer is what reveals if they care about the security of the computer or not.

In the context of this study attitudinal predispositions of cyber users towards secure cyber use explained whether they cared about security in IT or not since those who favored security were most likely to keep their data secured while those who disfavored security were most likely to use the Internet in way that expose their data to viruses. Consequently, the more confident a participant was towards using the Internet securely, the more positive their attitude was going to be towards Internet adoption and its related activities (Garland & Noyes, 2005).

Explanation and Manipulation of the Cybersecurity Awareness Training Variable

Research on cybersecurity (Dodge, Carver & Ferfuson, 2007; Eminağaoğlu, Ucar & Eren, 2009; Rezgui & Marks, 2008; Shaw, Chen, Harris, & Huang, 2009) identifies the importance of cybersecurity awareness training as an important activity that indicates if a cyber user has a positive or negative attitude towards Internet use and security. As observed in cybersecurity literature (Eminağaoğlu et al., 2009), having a positive attitude towards cybersecurity awareness training is an important operational trait that enhances security when using the Internet. This positive attitude towards cybersecurity training creates the much-needed security culture which, is critical for data availability, integrity, and confidentiality. The security training variable was conceptualized in the study as that formal or informal process that teaches cyber users on the security of their IT assets.

Security awareness training was operationally defined as a dichotomous variable with a “yes” or “no” response option. Participants answered yes or no to indicate if they have ever taken cybersecurity training. For those who responded yes, they were further required to indicate by the question: if they agreed that cybersecurity training was important with categories of strongly agree, somewhat agree, somewhat disagree,

strongly disagree. At the analysis level, the cybersecurity training variable was then cross-tabulated with the concern for cybersecurity variable to determine the relationship that both variables had with each other. The justification for this cross tabulation came from assertions in literature suggesting a relationship between cybersecurity awareness training and concern for cybersecurity (Rezgui & Marks, 2008).

The cybersecurity training variable was initially captured via the question: have you ever taken cybersecurity awareness training? The variable was also captured as a dichotomous variable with "Yes" and "No" response options as already indicated above. The yes or no answers clearly showed where the participant stood as far as the variable security awareness training was concerned.

Participants who reported to have taken security awareness training were further asked, if they agree that cybersecurity training was important? Options of strongly agree, somewhat agree, somewhat disagree, strongly disagree were given to help participants answer the question. Participants were also further asked to indicate the type of training they feel was important by providing the following training options: social engineering training, antivirus training, password management training, and others. All these categories identified a participants attitude towards cybersecurity awareness training and thus helped in analyzing and cross-tabulating each participant's response with concern for cybersecurity to determine if both variables had a relationship or not.

Justification for Including Security Awareness Training in the Analysis

As mentioned above a cyber user's attitudinal worldview towards security awareness training contributes to the overall security posture of a cyber environment as it determines whether the cyber user takes security training seriously or not thus reflecting

in the way they use the Internet. The necessity to develop a culture of security when dealing with IT systems is important because the security of the Internet is a collective endeavor because each user's actions affect other users (Dodge, Carver & Ferfuson, 2007). The actions of cyber users who fail to enforce security destroy the efforts of those who do especially when dealing with distributed denial-of-service (DDoS) attacks.

The 'human factor' input most collaborate with the technical input to provide the level of security that is sufficient to protect a network for people and technology must work together to secure a system. Since people play a significant role in enhancing security in an IT environment and are also one of the 'weakest links in the security chain' (Sasse & Flechais, 2005, p. 13), developing a positive attitude towards cybersecurity awareness training is important as it helps build a culture of security which, is needed for data availability, integrity and confidentiality. To adequately protect information assets, training must be considered important and cyber users must understand their roles and responsibilities while using the Internet, as well as follow security policies, procedures, and practices and the effect that those practices have on the overall security of the environment. All of this explains why security training was included in the analysis.

Explanation and Manipulation of the IT Savvy Variable

The IT savvy variable was operationally defined in the study as either a participant who is knowledgeable in using information technology systems or one who has operational knowledge of using computers or the Internet adequately. The IT savvy variable was captured in the research instrument through the question: Do you consider yourself IT savvy? Yes or no response options were given to help participants indicate if they considered themselves knowledgeable in using the Internet or not. A participant's

positive response to the IT savvy question was important because it indicated that the participant understood IT and its security as there is no adequate IT without security. The IT savvy question at the analysis level was equated with the concern for cybersecurity question in SPSS to determine if those who are IT savvy are concerned about the security of the Internet or not and if so how significant was the relationship.

Justification for Including the IT Savvy variable in the Analysis

The IT savvy variable was a foundational variable in the study because it helped identify a participant's comfort level in using IT thus giving them the confidence to proceed with the survey knowing that he or she is dealing with familiar territory. Since the study focused on understanding the relationship that exist between cyber usability and security, identifying that one was IT savvy established the fact that the participant would understand the questions and so answer them impartially and from the perspective of someone who has operational knowledge in IT thus helping to eliminate user's from skipping questions for lack of understanding for what the questions meant. The reason for including the IT savvy question could also be explained by the type of sample chosen for the study. The sample is composed of adult university students who use the Internet regularly. This sample assured the researcher that the participant's operational knowledge of IT would help them understand the questions and so participate enthusiastically and forthrightly. The IT savvy question at the analysis level was compared with the concern for security variable to understand if people who are comfortable in using the Internet are also concerned about the security of the Internet or not.

Explanation and Manipulation of the Type of Transaction Variable

The type of transaction variable was used in the research to understand if the type of business conducted on the Internet determined concern for security. The research asked the question, if the type of transaction conducted on the Internet determined concern for cybersecurity. Yes or no response options were given to help answer the question. The researcher then categorized the variable and asked participants the question to indicate one transaction they use the Internet for. The options given were: business transactions, financial transactions, educational transactions, family related transactions, and other.

Categorizing the business transaction variable in the research explained situations in which, a participant used the Internet for online shopping and related needs. Financial transactions covered cases where a study participant used the Internet to conduct online banking or money transfer operations. Educational transactions denoted a situation in which, a study participant used the Internet for online classes or research. Family related transactions covered a case in which, a study participant used the Internet to log in family related information like children's privacy information, family home addresses, marriage information, and date of birth, social security numbers, and others. Others covered all other transaction not explained above. At the analysis level the type of transaction variable was then compared with security to determine a relationship.

Justification for Including Type of Transaction in the Analysis

Determining the type of transaction carried out on the Internet was important because such information indicated if some online transactions demanded more security than others and if so why. Though it is important for all Internet related transactions to be

secure, the reality is that the nature of some web operations naturally demands higher security than others, especially those related to money or personally identifiable information. Although this is the natural presumption, scientific data is needed to justify this claim, thus highlighting why the type of transaction variable was necessary.

Explanation and Manipulation of the Financial Loss Variable

The financial loss variable was conceptually defined as the monetary cost suffered from a cyber breach. Literature on cybersecurity and the connection it has with financial assets suggests that higher levels of financial loss due to cyber breach have a positive relationship with users' concern for Internet security, and lower levels of financial losses have little or no relationship with the users' concern for Internet security (Acquisti, Friedman, & Telang, 2006). The variable was operationally defined as the amount of money one lost as a result of a cyber-attack. This definition of financial loss suggested that higher levels of financial loss were most likely to prompt Internet users to care more about security while using the Internet. Consequently, the more the amount of financial loss, the more concerned the victim was going to be about Internet security.

Financial loss data was first of all captured in the survey by giving participants the opportunity to indicate through yes or no answers if they have ever been victims of financial loss as a result of cybercrime. Participants who answered "yes" to this question implied a relationship and were then given the opportunity to indicate: what the associated financial cost they incurred as a result of the cyber breach was. Participants were then given dollar options of $0 to $999, $1.000 to $4.999, $5.000 to $10.000 to help them indicate the amount of money they lost due to a cyber-attack.

The identified dollar values were intended to help test the idea that large amounts of money lost due to a cyber hack would increase concern for cybersecurity as compared to low amounts of money lost due to a cyber-attack. At the analysis level, the associated financial cost variable was then equated with the concern for cybersecurity variable in SPSS to determine if the amount of money lost due to a cyber-attack determines concern for cybersecurity. As mentioned above, the rationale to crosstab security with the financial loss variable was to test the validity of the assertion that the more money a cyber user loses through a cybercrime the greater their concern towards Internet security.

Justification for Including Financial Loss in the Analysis

The rationale for including this variable in the analysis of the study emanated from the fact that literature (Acquisti, Friedman, & Telang, 2006) on cybersecurity explains the connections that past financial loss has on cyber users' level of concern for the security of the Internet. Financial loss as a result of a cyber-attack cost individuals and organizations in the United States alone billions of dollars in losses annually, and so it is appropriate to include the variable in the analytical models of the study to quantify at the micro level the connections it has on the cyber users who have experienced cyber breaches with resulting financial losses (Acquisti, Friedman, & Telang, 2006).

Explanation and Manipulation of the Level of Education Variable

According to the *Oxford Advanced Learners' Dictionary* (Hornsby, 2006), education is defined as a way of teaching and learning, especially in schools to improve knowledge and develop skills. The education variable was operationally defined to denote the academic degree any participant had acquired. This definition gave participants the opportunity to differentiate themselves from others using the level of

education categories. This was necessary as it also gave the researcher the ability to cross-tabulate the responses from each participant's degree level with their level of concern for Internet security with the aim of seeing if one's degree acquired or level of education had any relationship with their level of concern for Internet security.

The manipulation process of the variable required that the researcher categorizes the variable into an associate degree, bachelor's degree, master's degree, and doctoral degree. Associate degree and bachelor's degree categories covered college level students and in doing so helped justify Steve Jones' (2002) usage of this category in his prior study. The categories also gave the researcher the ability to cross-tabulate the responses vis-à-vis concern for Internet security with the aim of making a determination whether education level has any association with one's concern for Internet security.

Justification for Including Level of Education in the Analysis

Steve Jones asserted in his study—The Internet Goes to College, How Students are Living in the Future with Today's Technology—that 89% of college students do not only have a positive attitude towards secure Internet use but also use it first for their academic needs and also for personal and social needs more than their compatriots (Steve Jones, 2002). This calls not only for a justification of the assertion which, is intended but also helps question if education determines a cyber user's level of concern for security.

Explanation and Manipulation of the Gender Variable

Gender was operationally defined as a multi-category variable with three designated categories: male, female, and 'other.' This operational definition gave each survey participant the opportunity to identify and differentiate themselves from others according to their gender, thus underlining the connections that gender has on security

and giving a clear differentiation between masculinity and femininity. The categories male, female, and ‘other’ did not only further explain the variable but also gave the researcher the ability to distinguish one gender from the other. The category male was represented in the analysis as “a” female as “b,” and others as “c.” As a nominal variable, the gender categorizations were used by the researcher to determine if one’s sexual identity played any role in determining one’s level of concern for cybersecurity, thus indicating the level of association.

Justification for Including Gender in the Analysis

Right back in the 14th century, the word gender was used to define classes of nouns labeled as masculine, feminine, or neuter in some languages. This categorization of people as male and female represents sexual existence and recently has also included ‘other’ as those who identify themselves not to be male or female. Gender identity then refers to “one’s sense of oneself as male, female or transgender” (American Psychological Association, 2006, pp. 1-2).

In situations where gender identity and biological sex are not ‘consistent,' the individual may identify as ‘other’ meaning transsexual or any other gender which, is not male or female (Gainor, 2000). This characterization of people as male, female, and ‘other’ is part of reality and cannot be eradicated, thus justifying why it is relevant to this research. Downs, Ademaj, and Schuck (2009) found that men are more likely to be victims of cybercrime than women, which, justifies the need to explore further the role of gender in Internet use and security as well as the nature of relationships that exist therein.

Additionally, introducing the gender variable to the study was important because it helped test the validity of prior assertions from scholars like Bimber (2000), Hargittai

and Shafer (2006), and Ono and Zavodny (2003) who asserted that males compared to females have more knowledge about Internet security issues and not only update their anti-virus software more frequently but also use pop-up blockers when surfing the web. Gender did not only also differentiate research participants according to their sexual orientation but helped in the data analysis by cross-tabulating the gender variable with the concern for Internet security variable to see if the gender type of the cyber user determined their level of concern for Internet security or not.

Explanation and Manipulation of the Age Variable

The age variable was operationally defined in the study as simply the length of time a person has lived, or one's human existence which, is measured by years from birth. In a bid to better explain the variable and give respondents a better platform to respond, the researcher divided the variable into distinct age group categories. Responses from each age group were cross-tabulated with concern for Internet security to see if age has a relationship with one's concern for Internet security or not. The categorization of the age variable gave participants, who might not have wanted to identify their exact age and as a result skip the question, the opportunity to answer the question through the identification of themselves within the three defined age categories.

The age variable was identified in question 2 of the questionnaire and as already indicated was operationally defined and categorized into three groups namely: 18 to 30 which, represented younger age students, 31 to 50 which, served middle age students and 51 and older which, represented older age students. These age categorizations were used by the researcher to determine if one's age group had any relationship with ones level of concern for the security of the Internet or not.

Justification for Including Age in the Analysis

The rationale to include age in the study emanated from the fact that the researcher did not only wanted to understand if participants' level of concern for Internet security had any relationship with their age but also to test the validity of prior statements made by researchers on the connection age has on Internet use. According to Aaron Smith (2014), seniors in the United States historically are not only late in adopting and using technology securely compared to their younger compatriots but also need assistance using new technology, thus making them susceptible to cybercrime. This assertion necessitates justification, thus making the age variable necessary in the study.

Explanation and Manipulation of the Residence Variable

The residence of a cyber user was operationally defined in the research as the place where someone lives. This definition was further categorized into 'urban America' and 'rural America' to make it easy for participants to use residence to distinguish themselves from each other. This categorization was intentional because it gave the researcher the ability to make a determination if one's home location, domicile, or "zip code" had any relationship with their level of concern for cybersecurity.

According to Araque et al., although in the United States an estimated 85% of adults and more than 90% of teenagers use the Internet, some poorer areas of the country still see low rates of home computer use compared to others, and many languish without a connection to the web (Araque et al., 2012). This statement justified the importance of including the residence variable in the study as it would not only test the validity of the declaration but also explain whether high cybercrime rates in poor inner city neighborhoods could be associated with users' lack of familiarity with Internet security

requirements due to their inability to have and use the Internet. The categories also made it easy for the researcher to tabulate each participant's response on a table and cross-tabulate with their level of concern for Internet security to understand if age determined a cyber users level of concern for security.

Justification for Including Residence in the Analysis

The cyber user's residence location was used in the study for many reasons. The first reason was to test if the home location of a cyber user has any relationship with the user's level of concern for Internet security or not. The second reason was to test if the researcher's ideas on the relationship that a cyber user's home location has on their secure Internet use practice is correct or not. Answering these two questions was important as it would help state, local, and federal government officials allocate Internet resources equally in both the rural and urban parts of the country, and by doing so give citizens the opportunity to acquaint themselves with using the Internet securely for their needs.

Conclusion

In this chapter, an outline and justification of the methodological procedures used in data collection, treatment, and analysis were presented. Data utilized for the study was collected through a questionnaire which, was posted on SuveyMonkey and later exported to SPSS for analysis following the statistical models that were established for the study.

The operational definition of each variable used in the research highlighted what the research wanted to achieve and also justified the statistical technique that was used to explain and compare the variables in SPSS. The operational definition of the variables also laid the foundation for subsequent analysis in chapter four. In chapter four the focus

is directed on presenting, analyzing, and describing the crosstabs and presentations of data in contingency tables and well as the results of the statistical tests used in the study. Chi-square statistics identified the nature of the relationship while Lambda and Gamma identified the significance of the identified relationship.

Chapter 4: Data analysis and Presentation

Introduction

Before presenting and analyzing survey data, it is important to underscore the purpose of the study. The study explored attitudes of university students towards Internet utilization and security in the Washington, DC, area in an attempt to understand the type of relationship that exists between cyber utilization and cybercrime and then determine best practices that could help promote the secure use of the Internet.

Chapter four presents and analyzes the survey data collected through SuveyMonkey. To achieve this objective cross-tabulations, bar charts, Chi-square, Lambda, and Gamma tests were used to explain the value and statistical significance of the effects observed from the relationships between the variables. Cross-tabulations were equally used to test the research hypotheses to understand the nature of the relationship that exists between the independent and the dependent variables.

Cross-tabulations were used to show the distribution of the observations of the independent variables across the categories of the cases of the dependent variables. In the tables, the dependent variables appeared in columns while the independent variables appeared in rows. While analyzing the crosstabs, the occurrences of incidences of concern for Internet security were distributed across the categories of frequencies of occurrences of the independent variables.

Description of the Sample Used in the Study

The criteria for selecting the sample for this study included the following demographics: a) students who use the Internet, b) live in the Washington, DC, metro area, and c) fall between the ages of 18 and older. The study participants also came from

all walks of life, lived in the urban and rural areas of the Washington, DC, metro area, and included people of all genders and economic status.

The sample size consisted of 433 participants, and the questionnaire was disseminated to research participants via SuveyMonkey using judgment sample techniques. This was done by signing up and creating a professional plan with SuveyMonkey, identifying the criteria for participation in the study as well as the number of responses needed for the research, making payments for the project, and having SuveyMonkey generate and email the survey link to participants who met the stated criteria for the research. The survey was then closed when SuveyMonkey received the number of responses needed for the study.

Demographic and Descriptive Data

To paint a vivid picture of the population used for the research, the following demographic tables were created to describe the sample. Looking at the age Table 1 below, it is noticeable that 42.8% (185) of the participants fell between the ages of 31 to 50 years old, while the other 57.2% of the participants were split almost evenly between the younger and older groups: 29.9 % (129) between the ages of 18 to 30 years old, and 27.3% (118) ages of 51 and older.

Table 1

Age of Participants

How old are you?		Count	Column N %
How old are you?	18 - 30	129	29.9%
	31-50	185	42.8%
	51 and older	118	27.3%
	Total	432	100.0%

According to the Gender Table 2 below, it is evident that there were fewer male participants 44.0% (190), than females 55.1% (238). Just 0.9% (4) of the study participants fell into the 'other' category, meaning either lesbian, gay, bisexual, transgender, or queer.

Table 2

Gender Description

What is your gender?		Count	Column N %
What is your gender?	Male	190	44.0%
	Female	238	55.1%
	Other	4	0.9%
	Total	432	100.0%

From the level of education Table 3 below, it is evident that the sample of the study is highly educated. Fifty-six percent (242) of the study participants were students with master's degree, 5.3% (23) of the study participants were students with a doctoral degree, 29.4% had a bachelor's degree and 9.3% had an associate degree.

Table 3

Level of Education Description

What is your level of education?		Count	Column N %
What is your level of education?	Associate degree	40	9.3%
	Bachelor's degree	127	29.4%
	Master's Degree	242	56.0%
	Doctoral	23	5.3%
	Total	432	100.0%

Looking at the residence location Table 4 below, the majority 81% (349) of research participants are residents in the urban areas of Washington, DC, while only 18.8% (81) of the study participants live in the rural areas of the DC metro area.

Table 4

Residence Location Description

What is your residence location?		Count	Column N %
What is your residence?	Urban America	349	81.2%
	Rural America	81	18.8%
	Total	430	100.0%

Analysis of the Sample in Relation to the Responses on the Research Instrument

To lay the foundation needed for easy comprehension of the study results, it is important to perform an in-depth examination of the research sample population in comparison to the responses presented on the research instrument. The need to analyze the responses of the questionnaire before interpreting crosstabs in SPSS is because it helps us 1) explains eventual Lambda and Gamma effect values that will be obtained 2) rationalize the type of significance or strength of the results eventually obtained from Chi-square, lambda, and gamma testing; 3) explains expected cell count queries that may be raised in Chi-square; and 4) give clues of what participants feel about each question and the Internet security concern in question.

As a reminder, the focus of the study was to sample university students in the Washington, DC, area with the purpose of understanding attitudinal differences in Internet use and security, and understanding the relationship that cyber utilization have with cybercrime.

A closer look at the research instrument indicates a desire to understand the importance of Internet security using independent variables like cybersecurity awareness

training, being IT savvy, type of business conducted on the Internet, associated amount of financial loss from cybercrime, level of education, age, gender, and residence location.

Although some of the questions on the questionnaire were designed for emphasis purposes and therefore were not included in the cross-tabulation analysis in SPSS, they nonetheless revealed valuable pointers that link the study sample to the nature of results obtained even before the variables are compared with each other in SPSS.

Besides the fact that the research sample was chosen from an elite population, the question -*Do you consider yourself IT savvy?*—revealed that the sample population was also computer literate as 98.6% of participants indicated that they are IT savvy as can be seen in Table 5 below.

Table 5

Participants Indicating IT Savvy

Do you consider yourself IT savvy?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	426	98.4	98.6	98.6
	No	6	1.4	1.4	100.0
	Total	432	99.8	100.0	
Missing	System	1	.2		
Total		433	100.0		

This high percentage sets the stage for eventual justification of the study results. This justification is also solidified by the fact that 99.5% of the research participants also consider Internet security an important factor of their attitude towards cyber usability as indicated by the answers on Table 6 below.

Table 6

Participants Indicating Internet Security an Important Factor

Do you consider Internet security an important factor of your Internet use attitude?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	430	99.3	99.5	99.5
	No	2	.5	.5	100.0
	Total	432	99.8	100.0	
Missing	System	1	.2		
Total		433	100.0		

To support the fact that the sample was not only literate, computer savvy, and considered Internet security necessary, 93% of the sample indicated a favorable attitude towards security as there stated that they are highly concerned about cybersecurity as seen from the answers to Question 8 on the questionnaire and Table 7 below.

Table 7

Concern for Security Rating

Please rate your concern for security.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Little concerned	5	1.2	1.2	1.2
	Somewhat concerned	25	5.8	5.8	7.0
	Highly concerned	401	92.6	93.0	100.0
	Total	431	99.5	100.0	
Missing	System	2	.5		
Total		433	100.0		

It is also important to highlight from the responses to the question of *Please rate your concern for security* that, although 72.7% of the participants pointed out that they mostly use the Internet for financial transactions, 99.1% of them also felt that the type of transaction they mostly use the Internet for determined their concern for Internet security. Take a look on Tables 8 and 9 below.

Table 8

Internet Most Used for Which Transaction

From the list below, please indicate one transaction you mostly use the Internet for?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Other (please specify)	1	.2	.2	.2
	Business Transaction	70	16.2	16.2	16.4
	Financial Transactions	314	72.5	72.7	89.1
	Educational Transactions	17	3.9	3.9	93.1
	Family-Related Transaction	30	6.9	6.9	100.0
	Total	432	99.8	100.0	
Missing	System	1	.2		
Total		433	100.0		

Table 9

Internet Transaction Determines Concern for Internet Security

Does the type of transaction you mostly use the Internet for determine your concern for Internet security?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	428	98.8	99.1	99.1
	No	4	.9	.9	100.0
	Total	432	99.8	100.0	
Missing	System	1	.2		
Total		433	100.0		

Even before comparing the variables in SPSS, the above-obtained percentages from the responses to the questionnaire already indicate that study participants are concerned about security and have a favorable attitude towards security especially when using the Internet for financial transactions. This high percentage of concern for security when using the Internet for a financial transaction is justified by the fact that 94% of the participants indicated that they had been victims of cybercrime, especially computer virus with a 54.2% rate. Take a look at Tables 10 and 11 below.

Table 10

Participants Indicating Cybercrime or Scamming Victim

While using the Internet have you ever been a victim of cybercrime or scamming?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	406	93.8	94.0	94.0
	No	26	6.0	6.0	100.0
	Total	432	99.8	100.0	
Missing	System	1	.2		
Total		433	100.0		

Table 11

Type of Cybercrime Experienced

If yes what kind of cybercrime did you experience?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Embezzlement	3	.7	.7	.7
	Fraud	25	5.8	6.1	6.9
	Theft	115	26.6	28.2	35.0
	Computer Virus	221	51.0	54.2	89.2
	Sabotage	4	.9	1.0	90.2
	Denial of Service	5	1.2	1.2	91.4
	Breach of Computer systems	35	8.1	8.6	100.0
	Total	408	94.2	100.0	
Missing	System	25	5.8		
Total		433	100.0		

It is also important to underscore from the responses to the questionnaire that 97.7% of the study participants did not only acknowledge to have taken cybersecurity training but in doing so 68.4% of them strongly agreed that cybersecurity training is essential, especially anti-virus training with a 61.1% support rate to anti-virus training. Tables 12, 13, and 14 below indicate that clearly.

Table 12

Participants Indicating Cybersecurity Training

Have you ever taken cybersecurity training?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	418	96.5	97.7	97.7
	No	8	1.8	1.9	99.5
	Undecided	2	.5	.5	100.0
	Total	428	98.8	100.0	
Missing	System	5	1.2		
Total		433	100.0		

Table 13

Participants Indicating Cybersecurity Awareness Training as Important

Do you agree that cybersecurity awareness training is important?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	2	.5	.5	.5
	Somewhat disagree	9	2.1	2.1	2.6
	Somewhat agree	122	28.2	29.0	31.6
	Strongly agree	288	66.5	68.4	100.0
	Total	421	97.2	100.0	
Missing	System	12	2.8		
	Total	12	2.8		
Total		433	100.0		

Table 14

Type of Cybersecurity Awareness Training Considered Important

If you think cybersecurity awareness training is important, what type of training do you consider important?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Other (please specify)	7	1.6	1.7	1.7
	Social engineering training	136	31.4	32.1	33.7
	Anti-virus training	259	59.8	61.1	94.8
	Pass word management training	22	5.1	5.2	100.0
	Total	424	97.9	100.0	
Missing	System	9	2.1		
Total		433	100.0		

The responses obtained from the sample population portray participants who are educated, IT savvy, have a favorable attitude towards Internet security especially when using the Internet for financial transactions, and know the importance of cybersecurity awareness training and have equally taken the training themselves. These choices from the sample population would eventually determine the nature of the results of the study when the variables are compared with each other in cross-tabulation analysis and by so doing prosecute the case as to why it is necessary to continue researching this topic using different samples, variables, and methodologies.

Analysis and Interpretation of the Cross-Tabulations

The analysis and interpretation of the survey data were determined by the following goals: 1) to understand if a relationship exists between the study variables. 2) To determine the strength and meaning of the relationship. In order to achieve this task a

myriad of statistical tools were employed to test the relationship, and the choice of tests used was determined by the research design.

Considering that the variables were either nominal or ordinal, Chi-square and other nonparametric tests like Lambda and Gamma were used to verify the null hypothesis and examine data distributed in contingency tables. To make an efficient determination of statistical significance, a 95% confidence level was adopted leaving a 5% chance of error, thus establishing an alpha or p-value of 0.05. Such alpha level was acceptable because it minimized the risk of rejecting the null hypothesis in case it was true.

To highlight the objective of the study a recap of the research questions is given. This research study was designed to address the following questions.

RQ1. Is there a relationship between the users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity?

RQ2. Is there a relationship between the users considering themselves as IT savvy and their level of concern for cybersecurity?

RQ3. Is there a relationship between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity?

RQ4. Is there a relationship between amount of financial loss experienced due to cyber breach and level of concern for cybersecurity?

RQ5. Is there a relationship between the Internet user's educational level and their level of concern for cybersecurity?

RQ6. Is there a relationship between the Internet user's gender and their level of concern for cybersecurity?

RQ7. Is there a relationship between the Internet user's age and their level of concern for cybersecurity?

RQ8. Is there a relationship between the Internet user's residence location and their level of concern for cybersecurity?

Cross-Tabulation of Cybersecurity Awareness Training and Concern for Cybersecurity

The issue of noncompliance to information security policy is of primary concern to system owners and organizational leaders because of the danger it poses to data security. Cyber users' noncompliance to security has caused cyber leaders to invest enormous amounts of resources towards enhancing information security compliance. One of the ways proposed by scholars to solve the cyber-threat problem is cybersecurity awareness training, yet existing studies on the importance of training to promote information security policy compliance fail to utilize feedback from cyber users. This lack of input from cyber users has caused many cybersecurity awareness training programs to be ineffective in their quest to address the risk posed by security noncompliance (Puhakainen & Siponen, 2010).

The urgency of this issue explains why it was important to include the cybersecurity awareness training question in the survey that was presented to research participants. The security awareness training variable was also included to understand the role that training plays on security enforcement considering that some scholars argued that training was found to be a major determinant of enhanced security. The case processing summary table below was used to give an overview explanation of how many

participants answered the training and security questions and how many skipped the question. Take a look on the take below.

Table 15

Case Processing Summary Table of Cybersecurity Awareness Training and Concern for cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Do you agree that cybersecurity awareness training is important? * Please rate your concern for security.	422	97.5%	11	2.5%	433	100.0%

The above case processing summary Table 15 above highlights the valid, missing, and total cases of participation. From a total of 433 participants, 422 answered the question while 11 missing cases were recorded. Since the case processing summary table did not compare the variables, crosstabs were employed as seen via Table 16 below.

Table 16 below displays a crosstab of participants' views on the importance of cybersecuity awareness training and their concerns for information security. This analysis was considered relevant to this study because of the increasing role of cybersecuity awareness training in information security literature. In this regard the analysis was aimed at testing the notion that the higher a cyber-user considers cyber awareness training important the higher the user's concern will be for information security. 422 study participants responded to the questions on the importance of security awareness training and concern for information security. 95.5% (274) of the study participants who strongly agreed that cybersecuity awareness training was important were highly

concerned about the security of the Internet when browsing the web. 91.8 %(112) of the participants who somewhat agreed that cybersecuity awareness training was important were also highly concern about the security of the Internet when browsing the web. Interestingly, 76.9 %(10) of the participants who somewhat disagreed of the importance of cyber awareness training were highly concerned about the security of the Internet when browsing the web.

Drawing from these findings a conclusion was made that while Internet security is of critical importance to all cyber users, majority of the users who think highly of Internet security also consider important the need for cybersecuity awareness training. This finding corroborate the argument of some cyber scholars that security awareness training for IT users is critical to maintaining a secured information system ((Brodie, 2008; Eminağaoğlu et al., 2009; NIST, 1993).

Table 16

Contingency Table of Cybersecurity Awareness Training and Concern for Security.

Do you agree that cybersecurity awareness training is important? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
Do you agree that cybersecurity awareness training is important?	Somewhat disagree	Count	0	0	3	10	13
		% within Row	0.0%	0.0%	23.1%	76.9%	100.0%
		% within Column.	0.0%	0.0%	15.0%	2.5%	3.1%
	Somewhat agree	Count	1	2	7	112	122
		% within Row	0.8%	1.6%	5.7%	91.8%	100.0%
		% within Column.	100.0%	40.0%	35.0%	28.3%	28.9%
	Strongly agree	Count	0	3	10	274	287
		% within Row	0.0%	1.0%	3.5%	95.5%	100.0%
		% within Column.	0.0%	60.0%	50.0%	69.2%	68.0%
Total		Count	1	5	20	396	422
		% within Row	0.2%	1.2%	4.7%	93.8%	100.0%
		% within Column.	100.0%	100.0%	100.0%	100.0%	100.0%

To further analyze the results in graphical terms the below bar chart Figure 3 was produced to describe the distribution of the frequencies of the participants' views on the importance of cybersecurity awareness training and participants concerns for Internet security. The security awareness training variable could be found on the x-axis of the graph while the concern for security variable could be found on the y-axis of the graph. The graph corroborate the analysis presented in crosstabs above by highlighting that most cyber user's despite their cybersecurity training status feel that security is of concern to them when using the Internet. Take a look at the bar chart Figure 3 below.

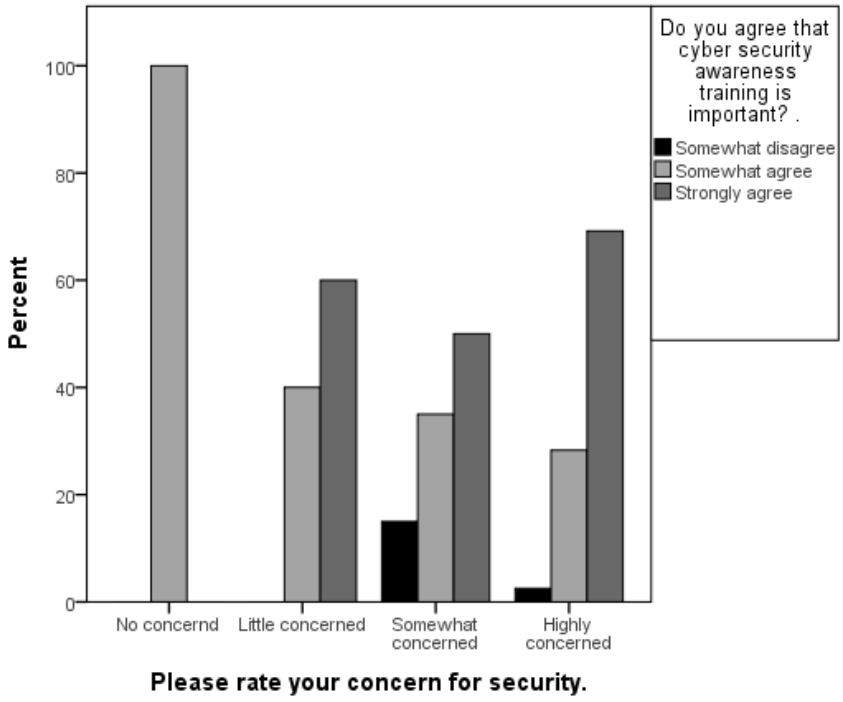

Figure 3. Cybersecurity awareness training and concern for security.

While the contingency table and the bar graph above analyzed and described participants' assessments of the type of relationship that exists between the variables, a robust analysis is, however, required to determine the level of statistical significance as well as the strength of significance. Test of statistical significance and strength of the relationship was established using Chi-square and the Lambda test of association. The

Pearson Chi-square test of independence represented by Table 17 below was configured in SPSS to check the level of statistical significance of the relationship between cybersecurity awareness training and concern for security. The relationship between these variables was significant as justified by the p-value of $p<.031$. The results indicated that there was evidence of a relationship between cybersecurity training and security.

The obtained *p*-value was below the accepted ideal alpha limit of .05. This finding justified the alternate hypothesis that supported the existence of a relationship between cybersecurity awareness training and concern for security. Based on this finding, the null hypothesis of this study was rejected. Here are the results below:

$$X^2 (6, N=422) = 13.839, p <.031.$$

Table 17

Pearson Chi-square Statistics of Cybersecurity Awareness Training and Concern for Security.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.839[a]	6	.031
Likelihood Ratio	9.608	6	.142
Linear-by-Linear Association	5.275	1	.022
N of Valid Cases	422		
a. 7 cells (58.3%) have expected count less than 5. The minimum expected count is .03.			

Although Chi-square test statistic showed evidence of a relationship between cybersecurity awareness training and concern for Internet security, there was nothing to suggest that the survey participants who had high concern for cybersecurity training also had high concern for Internet security. To test the strength of association, Lambda test statistics was employed. The Lambda Table 18 below produced a value of .006 which,

was considered to be too low to reduce error chances in confidently predicting that the same results could apply to other cases, thus suggesting a weak or insignificant relationship between the variables. Take a look on the Lambda Table 18 below.

Table 18

Lambda Test of Association of Variables

Directional Measures						
			Value	Asymptotic Standard Error	Approximate T[b]	Approximate Significance
Nominal by Nominal	Lambda	Symmetric	.006	.006	1.001	.317
		Do you agree that cybersecurity awareness training is important? Dependent	.007	.007	1.001	.317
		Please rate your concern for security. Dependent	.000	.000	.[c]	.[c]
	Goodman and Kruskal tau	Do you agree that cybersecurity awareness training is important? Dependent	.011	.007		.147[d]
		Please rate your concern for security. Dependent	.020	.022		.000[d]
a. Not assuming the null hypothesis.						
b. Using the asymptotic standard error assuming the null hypothesis.						
c. Cannot be computed because the asymptotic standard error equals zero.						
d. Based on chi-square approximation						

Cross-Tabulation of Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity

The IT savvy variable was important because it ensured that study participants were either knowledgeable or not knowledgeable about IT thus determining if they were comfortable participating in an IT related survey or not. The IT savvy variable also helped explain if being IT savvy necessarily connects to being concerned about security

when using the Internet or not. In order to understand if participants were knowledgeable in IT or not a question was asked: Do you consider yourself IT savvy? Participants were given yes or no options to help answer the question. Responses from the IT savvy question were then compared with responses to the concern for security question in SPSS to understand how related both variables were. Crosstabs were produced to describe the observed relationship, while Chi-square analysis was used to explain the significance of the relationship. The case processing summary table below was used to give an overview picture of how many participants took part in the survey and how many either answered or omitted the question.

Table 159

Case Processing Summary Table of Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Do you consider yourself IT savvy? * Please rate your concern for security.	432	99.8%	1	0.2%	433	100.0%

The above case processing summary Table 19 indicates that out of a total of 433 survey participants, 99.8% (432) actually answered the question while a 0.2% (1) missing rate was recorded. Since the job of the case processing summary table was not to explain the results obtained from comparing the variables with each other, a more robust cross-tabulation test was needed to reveal what happens when the variables are equated with each other in contingency tables. Take a look on the crosstab Table 20 below.

Table 20

Contingency Table of Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity

Do you consider yourself IT savvy? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
Do you consider yourself IT savvy?	Yes	Count	1	5	24	396	426
		% within Row	0.2%	1.2%	5.6%	93.0%	100.0%
		% within Column.	100.0%	100.0%	96.0%	98.8%	98.6%
	No	Count	0	0	1	5	6
		% within Row	0.0%	0.0%	16.7%	83.3%	100.0%
		% within Column.	0.0%	0.0%	4.0%	1.2%	1.4%
Total		Count	1	5	25	401	432
		% within Row	0.2%	1.2%	5.8%	92.8%	100.0%
		% within Column.	100.0%	100.0%	100.0%	100.0%	100.0%

Table 20 above displays a crosstab of what participants feel about being IT savvy and their concerns for information security. This analysis was considered relevant because of the necessity for cyber users to be IT savvy before using the computer. These analyses focused on testing the view that cyber users who are IT savvy have more concern for security when using the Internet than those who are not. 432 participants responded to the questions on being IT savvy and concern for information security. 93.0% (396) of the study participants who affirmed to be IT savvy also indicated that they were highly concerned about security when browsing the web. Only 0.2% (1) of participants who indicated that they were IT savvy said that they had no concern for security when using the Internet. 83.3% (5) of participants who were not IT savvy also

said that they were highly concerned about security. None of the participants who were not IT savvy said that they had no concern for security when browsing the web.

Although crosstabs compared the variables, the results were not presented in chart format. To create a graphic image of the relationship, the SPSS graphical representation was configured to produce the bar graph in Figure 4 below. The independent variable was placed on the x-axis of the graph while the dependent variable was placed on the y-axis.

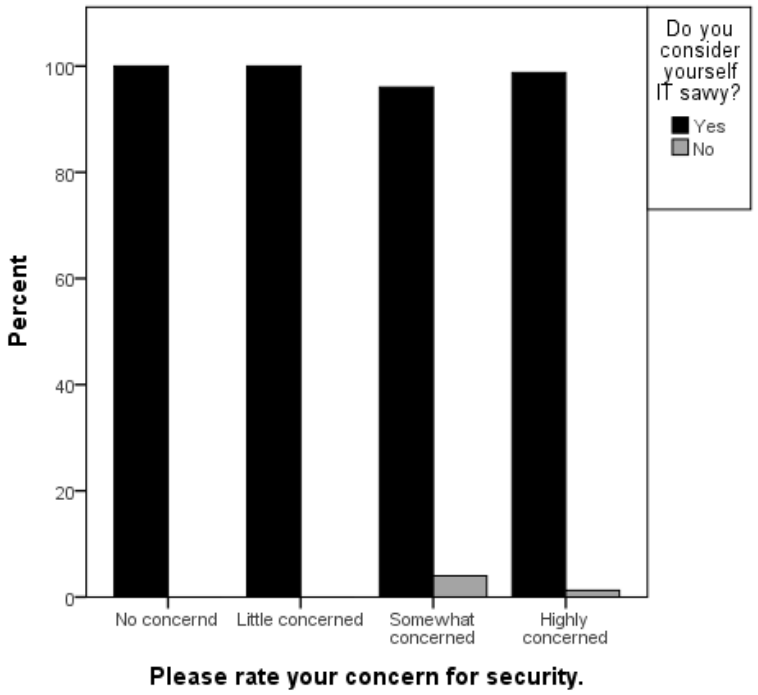

Figure 4. Cyber User's Considering Themselves as IT Savvy and Concern for Cybersecurity.

The bar chart results represented by Figure 4 above validate the crosstab results in stating that majority of participants irrespective of whether they considered themselves IT savvy or not were highly concerned about security in IT.

It is important before analyzing the strength and direction of the results to examine scholars' views on low expected cell count in Chi-square. This analysis is

necessary and explains all situations where Chi-square warns of low expected cell count in the study. Literature approaches the issue of low expected cell count in Chi-square from conflicting views, and so scholars like Cochran (1954) maintain overly conservative guidelines on the issue by insisting that low expected cell counts in Chi-square are unacceptable in all cases. Although Cochran's concerns align with the assumptions of Chi-square, researchers like Agresti (1990) contend that such stipulations not only intricate but improbable to expect a single rule to explain all cases since studies with large sample sizes, like in this study, still sometimes have expected cell count warnings, thus justifying why some researchers don't find that too problematic (Agresti, 1990; Cochran, 1954).

In addition, Conover (1999) aligns with Agresti and argues that Cochran's "rule of thumb" on expected cell count size is not only overly conservative but fails to acknowledge that expected count size can be "as small as 0.5, as long as most are greater than 1.0, without endangering the validity of the test" (Conover, 1999, p. 202; see also Cochran, 1954; Agresti, 1990). Cochran, who is noted to be a staunch supporter of high expected cell counts levels in Chi-square, has relaxed his rule by saying that as long as the expected count is less than 1 Chi-square, results are valid (1954). Notwithstanding these views, the SPSS Fisher's Exact Test module is used by some researchers to explain Chi-square *p* value in situations where sample size is low which, is not true in this case.

The Pearson Chi-square test of independence seen below in Table 21 was also configured in SPSS to verify the level of statistical significance of the relationship between being IT savvy and having concern for security. The relationship between these variables was not significant as shown by the asymptotic significance value of *p* .708.

The obtained p-value of *p* .708 was above the accepted alpha limit of .05. This finding did not justify the alternate hypothesis that there is a statistical relationship between being IT savvy and having concern for security. Therefore the alternate hypothesis was rejected and the null accepted since there was evidence that there was no relationship between being IT savvy and having concern for security. Being IT savvy was not a necessary condition for having concern for security. Here are the results below:

$$X^2 (3, N=432) = 1.388, p .708.$$

Table 21

Pearson Chi-square Statistics of Concern for Security and Cyber User's Considering Themselves as IT Savvy.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.388[a]	3	.708
Likelihood Ratio	1.056	3	.788
Linear-by-Linear Association	.321	1	.571
N of Valid Cases	432		
a. 5 cells (62.5%) have expected count less than 5. The minimum expected count is .01.			

Cross-Tabulation of Type of Transaction One Uses the Internet for and Concern for Cybersecurity

While most scholars in the field agree on the importance of Internet security for effective cyber use, some argue that certain transactions command more security than others. To explain whether the type of transaction conducted on the Internet determines a cyber user's level of concern for security, the type of transaction variable was included as one of the independent variables to be tested in the study. It should be mentioned that, proponents of the payment card industry (PCI) and the Sarbanes Oxley (SOX) law have a

particular favor on promoting tight security for Internet users conducting financial transactions. Despite the fact that such views seem reasonable, they necessitate empirical testing since security cannot be undermined for some Internet transactions simple because there are not money related.

To understand the relationship that exists between the type of transaction conducted on the Internet and concern for security, it was important to include the type of Internet transaction question on the questionnaire for the survey. After receiving 433 responses adequate for the study, data was exported from SuveyMonkey to SPSS for analysis. The type of transaction variable appeared in rows while the concern for security variable appeared in columns. From the case processing summary table 22 below, a 99.5% (431) valid response rate was recorded followed by a 0.5% (2) missing rate. Here are the results.

Table 162

Case Processing Summary Table of Type of Transaction One Uses the Internet for and the Concern for security.

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Please indicate one transaction you mostly use the Internet for? * Please rate your concern for security.	431	99.5%	2	0.5%	433	100.0%

Considering the fact that the case processing summary table only gave an overview of how participants responded to the type of transaction and the concern for

security questions, it was necessary to compare both variables to understand how related there are. Cross-tabulation analysis was then employed to help equate the variables.

Looking at the crosstab Table 23 below, certain capstones are noticeable. Out of the 431 participants who answered the questions, 97.1% (68) of the participants who identified business transaction as the type of transaction they mostly use the Internet for also indicated that they were highly concerned about security. 92.7% (291) participants who identified financial transaction as the type of transaction they mostly use the Internet for also indicated that they were highly concerned about security. 70.6% (12) of the participants who identified educational transaction as the type of transaction they mostly use the Internet for also indicated that they were highly concerned about security. 96.7% (29) who indicated to mostly use the Internet for family related transaction also showed that they were highly concerned about security.

No participant from the business, financial, and family related transaction categories indicated that they were not concerned about security when using the Internet. Only 1 participant from the educational transaction category indicated that security is not of concern to them when conducting business on the Internet. From the total percentages, it would be right to argue that majority of participants thought that Internet security is important to them irrespective of the type of transaction they use the Internet for. Take a look on the crosstab table 23 below to see the results.

Table 173

Contingency Table of Type of Transaction One Uses the Internet for and concern for security.

Please indicate one transaction you mostly use the Internet for? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
Please indicate one transaction you mostly use the Internet for?	Business Transaction	Count	0	1	1	68	70
		% within Row?	0.0%	1.4%	1.4%	97.1%	100.0%
		% within Column.	0.0%	20.0%	4.0%	17.0%	16.2%
	Financial Transactions	Count	0	4	19	291	314
		% within Row?	0.0%	1.3%	6.1%	92.7%	100.0%
		% within Column.	0.0%	80.0%	76.0%	72.8%	72.9%
	Educational Transactions	Count	1	0	4	12	17
		% within Row?	5.9%	0.0%	23.5%	70.6%	100.0%
		% within Column.	100.0%	0.0%	16.0%	3.0%	3.9%
	Family - Related Transaction	Count	0	0	1	29	30
		% within Row?	0.0%	0.0%	3.3%	96.7%	100.0%
		% within Column.	0.0%	0.0%	4.0%	7.3%	7.0%
Total		Count	1	5	25	400	431
		% within Row?	0.2%	1.2%	5.8%	92.8%	100.0%
		% within Column.	100.0%	100.0%	100.0%	100.0%	100.0%

The above tables compared the variables but did not represent the results in graphical format. To give a graphical analysis of the relationship, SPSS was also configured to generate the bar chart below. The independent variable appeared on the x-axis of the graph while the dependent variable appeared on the y-axis of the graph. Looking at the bar graph in Figure 5 below, it is evident that the results substantiate the analysis presented in the contingency table above and point to the fact that majority of participants admitted that Internet security was of concern to them and not necessarily determined by the type of transaction conducted on the Internet.

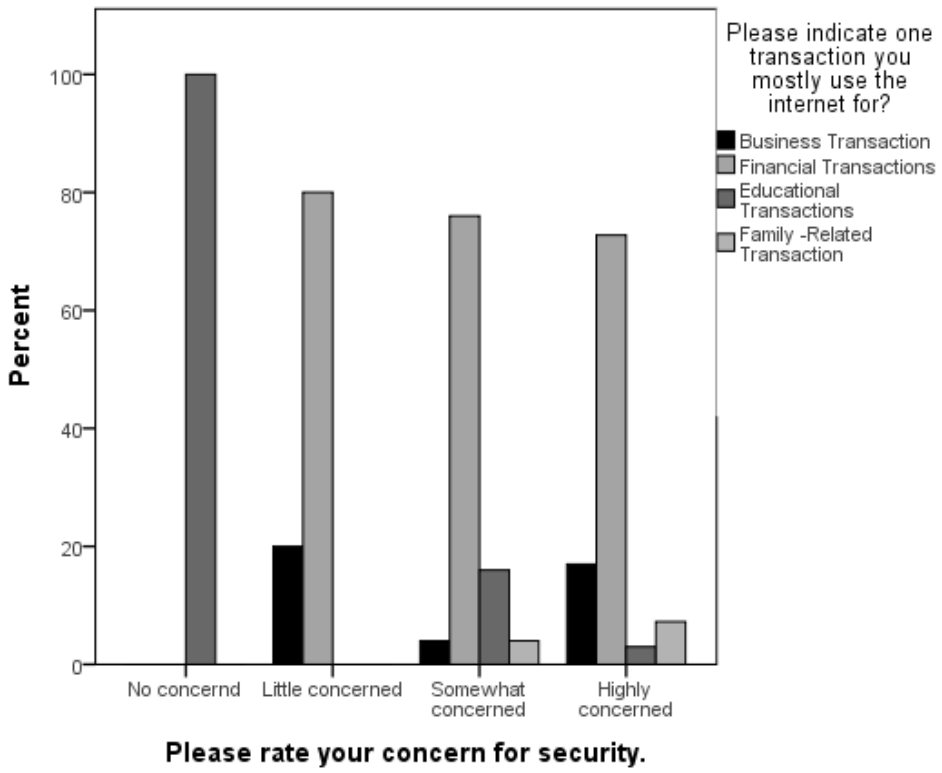

Figure 5. Type of transaction you use the Internet for and Concern for security.

To understand if the variables had a relationship or not Chi-square test of independence represented by Table 24 below was conducted. The Pearson Chi-square results indicated that there was evidence of a relationship as confirmed by the asymptotic significance value of p<.001. The obtained value of p<.001 was below the stated theoretical .05 p-value of the study, thus showing evidence of the existence of a relationship between the variables. Therefore, the alternate hypothesis was accepted, and the null hypothesis rejected. Here are the results:

$$X^2 (9, N=431) = 37.939, p < .001.$$

Table 24

Pearson Chi-square Statistics of Type of Transaction One Uses the Internet for and Concern for Security.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	37.939[a]	9	.000
Likelihood Ratio	17.704	9	.039
Linear-by-Linear Association	1.189	1	.276
N of Valid Cases	431		
a. 11 cells (68.8%) have expected count less than 5. The minimum expected count is .04.			

Pearson Chi-square test statistic determined evidence of a relationship but did not confirm the significance or strength of the obtained relationship. To determine the strength of association of the variables Gamma test statistics represented by Table 25 below was employed. The obtained Gamma value of .297 was low indicating a weak relationship. This insignificant relationship increased the chances of committing an error if a prediction of a relationship was made between type of transaction and concern for security in all cases. Take a look at the Lambda table 25 below:

Table 25

Gamma Test of Association of the Variables

Symmetric Measures					
		Value	Asymptotic Standard Error	Approximate T[b]	Approximate Significance
Nominal by Nominal	Phi	.297			.000
	Cramer's V	.171			.000
Ordinal by Ordinal	Gamma	-.353	.156	-1.973	.049
N of Valid Cases		431			
a. Not assuming the null hypothesis.					
b. Using the asymptotic standard error assuming the null hypothesis.					

Cross-Tabulation of Concern for Security and Associated Financial Cost Incurred from Cyber breach

Scholars have argued that the amount of money lost due to a cyber hack defines how concerned a cyber user would be about the security of the Internet. These views probably emanate from the notion that cyber users who lose more money from a cyber scam are more concerned about security compared to those who lose less money. Although this view seems reasonable, it might not necessarily be true in all cases, thus necessitating empirical testing. To understand the type of relationship that could exist between associated financial costs incurred through cybercrime and Internet security, the financial cost variable was included among the independent variables tested in the study.

Data were collected via SuveyMonkey and exported to SPSS for analysis. The case processing summary table seen below was first configured via SPSS to give an overview of how participants answered both questions. Take a look on table 26 below.

Table 26

Case Processing Summary Table of Associated Financial Cost Incurred due to Cyber breach and Concern for Security

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What was the associated financial cost incurred due to cyber breach? * Please rate your concern for security.	392	90.5%	41	9.5%	433	100.0%

From the above case processing summary Table 26, the valid, missing, and total cases are presented. Out of a total of 433 participants who took part in the survey, 90.5% valid cases were recorded while 9.5% missing cases were noted. Since the case processing summary table only gave an overview picture of how participants answered both questions, it was necessary to run cross tabulation analysis to understand what happens when both variables are compared with each other in SPSS. Take a look at the crosstab table 27 below.

Table 27

Contingency Table of Associated Financial Cost Incurred due to Cyber breach and Concern for Security

What was the associated financial cost incurred due to cyber breach? * Please rate your concern for security.						
			Please rate your concern for security.			
			Little concerned	Somewhat concerned	Highly concerned	Total
What was the associated financial cost incurred due to cyber breach?	$0-$999.00	Count	4	17	344	365
		% within Row	1.1%	4.7%	94.2%	100.0%
		% within Column.	80.0%	94.4%	93.2%	93.1%
	$1000-$4999	Count	1	1	20	22
		% within Row	4.5%	4.5%	90.9%	100.0%
		% within Column.	20.0%	5.6%	5.4%	5.6%
	$5000-$10.000	Count	0	0	5	5
		% within Row	0.0%	0.0%	100.0%	100.0%
		% within Column.	0.0%	0.0%	1.4%	1.3%
Total		Count	5	18	369	392
		% within Row	1.3%	4.6%	94.1%	100.0%
		% within Column.	100.0%	100.0%	100.0%	100.0%

From the contingency Table, 27 above some high water marks are observed. Out of the 392 participant who answered both questions, 94.2% (344) of the participants who indicated to have lost between 0 and 999 dollars as a result of a cyber-attack also

indicated that they were highly concerned about security. 90.9% (20) of the participants who indicated to have lost between 1000 to 4999 dollars as a result of a cyber scam also indicated that they were highly concerned about the security of the Internet. 100% (5) of the participants who indicated to have lost between 5000 and 10.000 dollars as a result of a cyber scam also indicated that they were highly concerned about security when using the Internet. No participant who lost between 5000 and 10.000 indicated that they had little concern for security. Only 1 participant who lost between 1000 to 4999 dollars and 4 participants who lost between 0 to 999 dollars indicated that they had little concern for security when using the Internet. From the total percentages majority of participants felt that Internet security is a key component of their Internet use practice irrespective of the amount of financial loss they have incurred from a cyber scam.

However, what was not evident was the idea that the more money one loses as a result of cybercrime, the greater their concern for security or the idea that loss of money through cybercrime causes lack of concern for security. These questions were not answered because the scope of the study was not designed to respond to such questions. Nonetheless, that is an interesting question to be answered in future inquiries.

To further analyze the results in graphical terms, the bar chart below was produced to describe the distribution of the frequencies of the participants' views on concern for security vis-à-vis the amount of financial cost incurred from cybercrime. The independent variable of the study was placed on the x-axis of the graph while the dependent variable was placed on the y-axis of the graph. Take a look at the bar chart Figure 6 below.

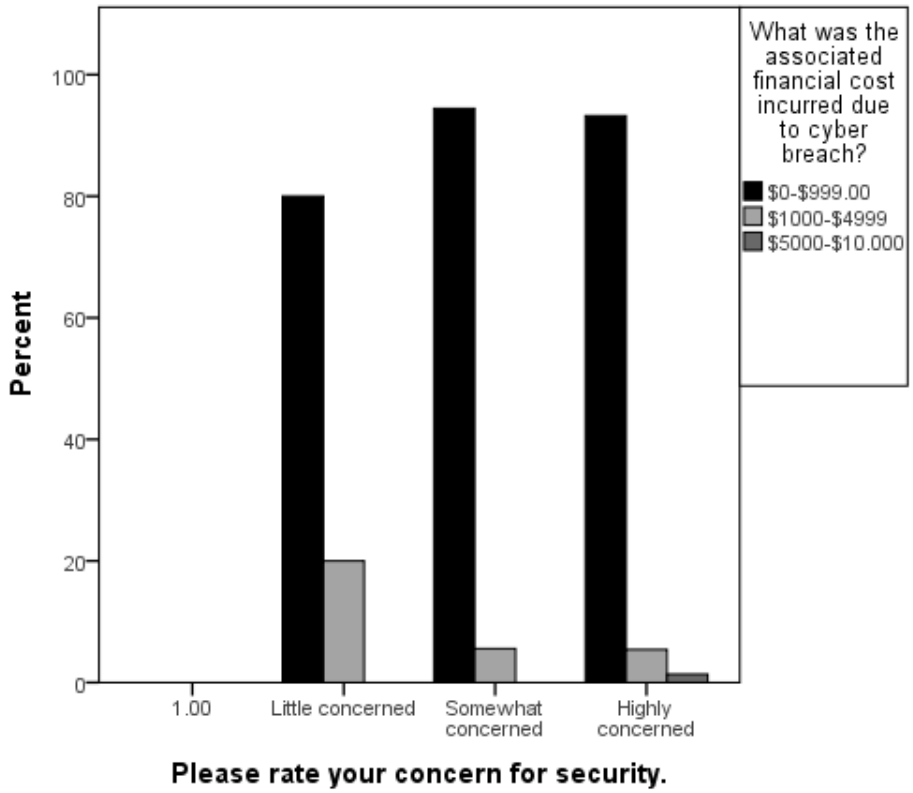

Figure 6. Concern for security and Associated Financial Cost Incurred due to Cyber breach.

From the above bar chart, it is evident that the results confirm the analysis presented in contingency tables and point to the fact that majority of participants consider Internet security important irrespective of the amount of money lost as a result of a cyber scam.

IT should be indicated that the crosstabs and bar graphs did not reveal if a relationship existed or not and if so how significant was the relationship. To understand if a relationship existed or not and also the significance of the relationship, Chi-square test of independence was conducted. Take a look at the Chi-square Table 28 below.

Table 28

Pearson Chi-square Associated Financial Cost Incurred due to Cyber breach and Concern for Security

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.277[a]	4	.685
Likelihood Ratio	1.833	4	.766
Linear-by-Linear Association	.141	1	.708
N of Valid Cases	392		
a. 6 cells (66.7%) have expected count less than 5. The minimum expected count is .06.			

The above Pearson Chi-square test of independence was conducted to understand the relationship between associated financial cost incurred from cybercrime and participants' views on concern for Internet security. The relationship between these variables was not significant as justified by the Chi-square asymptotic significance value of .685. This obtained value was higher than the stated p-value of .05, thus justifying the necessity to accept the null hypothesis and reject the alternate hypothesis of the study. Here are the results:

$$X^2\ (4, N = 392) = 2.277, p = .685.$$

Cross-Tabulation of Level of Education and Concern for Internet Security

The level of education variable was included in the study to understand if a cyber user's academic qualification plays any role in determining if the user has concern for the security of the Internet or not. To accomplish this task a survey was taken via SuveyMonkey and responses were received from a sample of 433 participants. Survey results were then exported to SPSS for analysis. The case processing summary Table 29

below gives a rundown of participants' responses regarding the level of education variable and the concern for security variable.

Table 29

Case Processing Summary Table of Level of Education and Concern for Cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What is your level of education? * Please rate your concern for security.	432	99.8%	1	0.2%	433	100.0%

Table 29 above presents an overview of the valid, missing, and total cases of how participants responded to the level of education and concern for security questions. Out of a total sample of 433 participants used for the study, 432 valid cases were recorded while a 0.2% missing case was identified. The case processing summary table did not proceed to analyze and compare participant's views on the relationship that exist between the educational level and concern for cybersecurity. To understand what happens when both variables are equated with each other in SPSS, cross-tabulation analysis was employed. Take a look at the crosstab results below in Table 30.

Table 30

Contingency Table of Level of Education and Concern for Cybersecurity

What is your level of education? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
What is your level of education?	Associate degree	Count	0	2	3	35	40
		% within row	0.0%	5.0%	7.5%	87.5%	100.0%
		% within column	0.0%	40.0%	12.0%	8.7%	9.3%
	Bachelor's degree	Count	1	2	8	116	127
		% within row	0.8%	1.6%	6.3%	91.3%	100.0%
		% within column	100.0%	40.0%	32.0%	28.9%	29.4%
	Master's degree	Count	0	1	14	227	242
		% within row	0.0%	0.4%	5.8%	93.8%	100.0%
		% within column	0.0%	20.0%	56.0%	56.6%	56.0%
	Doctoral degree	Count	0	0	0	23	23
		% within row	0.0%	0.0%	0.0%	100.0%	100.0%
		% within column	0.0%	0.0%	0.0%	5.7%	5.3%
Total		Count	1	5	25	401	432
		% within row	0.2%	1.2%	5.8%	92.8%	100.0%
		% within column	100.0%	100.0%	100.0%	100.0%	100.0%

The above cross-tabulation Table 30 displays the outcome of what happens when the level of education variable is compared with the concern for security variable in SPSS. The concern for cybersecurity variable was placed in the columns of the crosstab table while the level of education variable was placed in the rows of the table. The level of education question in the study was conceptualized as a quadrant with four nominal categories: associate degree, bachelor's degree, master's degree, and doctoral degree. The concern for cybersecurity variable was conceptualized into four categories of highly concerned, somewhat concerned, little concerned and no concerned.

Looking at the contingency table, some peak numbers are noticeable. Out of a total of 432 participants who answered the question, 87.5% (35) of participants with

associate degree were highly concerned about security when using the Internet. 91.3% (116) of participants with bachelor's degree were highly concerned about security when using the Internet. 93.8% (227) of research participants with master's degree indicated that they were highly concerned about security when using the Internet. 100.0% (23) of research participants with doctoral degree showed that they were highly concerned about security when using the Internet. No (0.0%) participant with associate degree, master's degree and doctoral degree indicated that they had no concern for security when using the Internet. Only 1 (0.8%) participant with bachelor's degree had no concern for security when using the Internet.

From the crosstab results, it is clear that a greater majority of the participants irrespective of their level of education category indicated that they are highly concerned about security when using the Internet. However, it would have been interesting to compare and see if uneducated people would also think same of Internet security but that was not within the scope of the study and would be an interesting recommendation for a future study.

It is important to indicate that the cross-tabulation table displays a frequency distribution of so many cases and values for each variable which, makes it difficult to immediately identify the percentages that indicate important relationships between variables. To create a snapshot of the relationship that exist between the level of education variable and the concern for cybersecurity variable in pectoral form, SPSS was configured to generate the bar chart Figure 7 below. The education variable appeared on the x-axis of the graph while the cybersecurity variable appeared on the y-axis of the graph. Take a look on Figure 7 below.

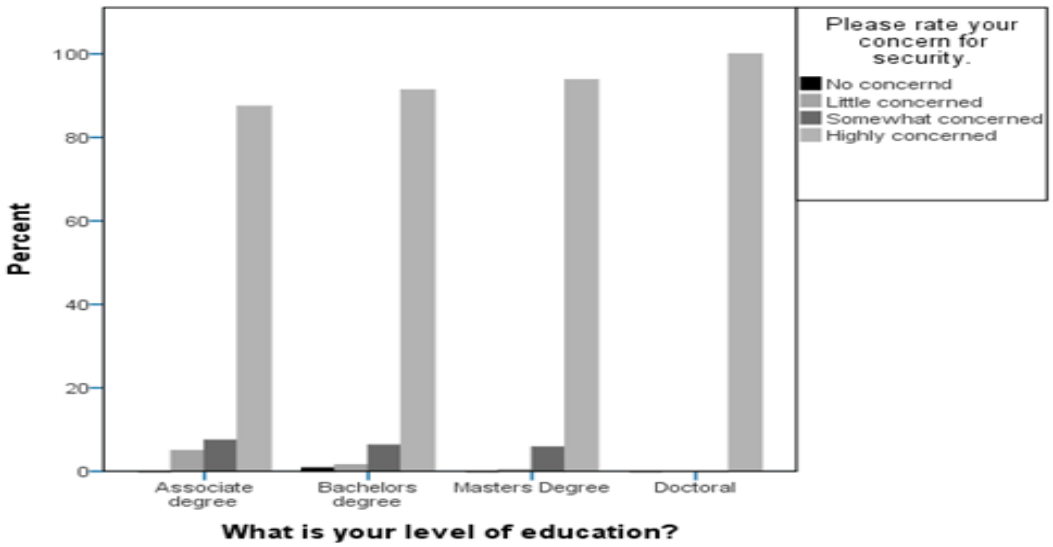

Figure 7. Bar chart on level of education and concern for cybersecurity.

Looking at the bar graph, it is evident that the results corroborate the analysis presented in the crosstabs above. Majority of participants irrespective of the level of education category indicate that they are concerned about security when using the Internet. Concern or non-concern for Internet security does not depend on the level of education of the person using the Internet as the security of the Internet is important to cyber users irrespective of their academic qualification.

Table 18

Pearson Chi-square Statistics of Level of Education and Concern for Cybersecurity.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11.016[a]	9	.275
Likelihood Ratio	10.681	9	.298
Linear-by-Linear Association	6.032	1	.014
N of Valid Cases	432		
a. 10 cells (62.5%) have expected count less than 5. The minimum expected count is .05.			

The Pearson Chi-square test of independence seen above on Table 31 was configured in SPSS to verify the existence or non-existence of a relationship between the

variables. The Chi-square results were not significant as shown by the p-value of .275. These results suggest that the cyber user's level of education does not have a relationship with their level of concern for cybersecurity. The obtained p-value falls above the accepted alpha limit of .05. This finding does not justify the alternate hypothesis that education has a relationship with concern for cybersecurity. Based on this finding, the null hypothesis of this study is accepted and the alternate hypothesis is rejected. Here are the results below:

$$X^2 \ (9, N=432) = 11.016, p = .275.$$

Cross-Tabulation of Gender and Concern for Cybersecurity

While scholars agree that gender pays a role in determining whether or not a cyber user has concern for security when browsing the Internet, they are not clear on the nature of the relationship. To understand such detail, gender was included as one of the independent variables to be tested in the study. The gender variable was conceptualized as a nominal variable with three categories: male, female, and 'other'. Participant's responses on the gender and concern for security questions were equated with each other in SPSS. The case processing summary table generated by SPSS briefly describes how participants responded to the gender and concern for security question while the crosstab table highlights what happens when both variables are paralleled with each other in contingency tables. Looking at the case processing summary Table 32 below, a snapshot of the valid, the missing, and the total number of cases of participation is revealed. The table indicates that out of a total of 433 participants who took part in the study, 432 valid cases were recorded while 1 case was missing. Take a look at Table 32 below.

Table 192

Case Processing Summary Table of Gender and Concern for Cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What is your gender? * Please rate your concern for security.	432	99.8%	1	0.2%	433	100.0%

Since the above case processing summary Table 32 only gives an overview of participant's responses on gender and concern for security, SPSS was configured to give a robust comparison of the variables in contingency tables. The concern for security variable was placed in the columns of the table while the gender variable was placed in the rows of the crosstab table. Looking at the cross-tabulation Table 33 below, some peak numbers are noticeable. Out of the 432 survey participants who answered the gender and concern for cybersecurity question, 92.1% (175) of male participants were highly concerned about security while 93.3% (222) of female participants were highly concerned about security. 100.0 % (4) participants from the 'other' category were highly concerned about security when using the Internet.

No (0.0%) participant from the male and 'other' categories indicated that they had no concern for security when using the Internet. 1 (0.4%) female participant indicated that they had no concern for security when using the Internet. The crosstab results summarily indicate that majority of participants irrespective of their gender category were highly concerned about security when using the Internet. Take a look at the contingency table 33 below.

Table 203

Contingency Table of Gender and Concern for Cybersecurity

What is your gender? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
What is your gender?	Male	Count	0	2	13	175	190
		% within row	0.0%	1.1%	6.8%	92.1%	100.0%
		% within column	0.0%	40.0%	52.0%	43.6%	44.0%
	Female	Count	1	3	12	222	238
		% within row	0.4%	1.3%	5.0%	93.3%	100.0%
		% within column	100.0%	60.0%	48.0%	55.4%	55.1%
	Other	Count	0	0	0	4	4
		% within row	0.0%	0.0%	0.0%	100.0%	100.0%
		% within column	0.0%	0.0%	0.0%	1.0%	0.9%
Total		Count	1	5	25	401	432
		% within row	0.2%	1.2%	5.8%	92.8%	100.0%
		% within column	100.0%	100.0%	100.0%	100.0%	100.0%

Although crosstabs compared the variables by analyzing the type of relationship that exist between gender and participants level of concern for the security of the Internet, the results were not presented in graphical format making it difficult to quickly identify the percentages that highlight important relationships. To create a graphical representation of the results, SPSS was configured to produce a bar chart of the relationship. The independent variable ‘gender’ appeared on the x-axis of the graph while the cybersecurity variable appeared on the y-axis of the graph. Looking at the bar graph figure below, it is clear that the results support the analysis presented in cross-tabs above. The bar graph validates the fact that almost all participants are concerned about Internet security irrespective of their gender category. Take a look on Figure 8 below to see the bar chart of the relationship.

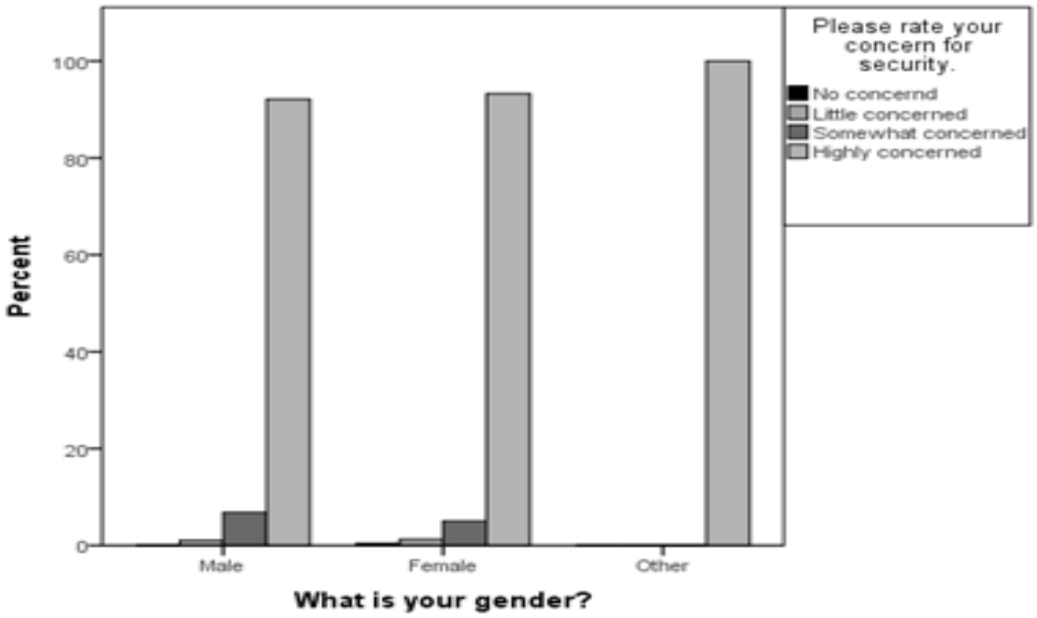

Figure 1. Gender and concern for cybersecurity.

Considering the fact that cross-tabulation analysis did not explain statistical significance of the variables, the Pearson Chi-square test of independence represented by Table 34 below was performed to test for statistical significance between gender and the concern for security. The relationship between the variables was not significant indicating evidence of no connection between gender and concern for security. These results indicate that participants' level of concern for the security of the Internet either cannot be explained and separated along gender lines or does not depend on a cyber user's gender. The Chi-square asymptotic significance value of .940 was higher than the stated p-value of 0.05. Here are the results.

$$X^2 \ (6, N=432) = 1.765, p = .940$$

Considering that the p-value of .940 was higher than the theoretical p-value of 0.05 stated for this study, a conclusion was made that there was evidence of no relationship between gender and concern for security. This conclusion justified the null

hypothesis when it contends that the gender of the cyber user has no connection with the user's level of concern for the security of the Internet. Based on this conclusion, the proposition of the alternate hypothesis was rejected.

Table 214

Pearson Chi-square Statistics of Gender and Concern for Cybersecurity

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.765[a]	6	.940
Likelihood Ratio	2.409	6	.879
Linear-by-Linear Association	.030	1	.861
N of Valid Cases	432		
a. 8 cells (66.7%) have expected count less than 5. The minimum expected count is .01.			

Cross-Tabulation of Age and the Importance of Internet Security

The age variable was included in the study to explain if older cyber users are more concerned about security when using the Internet than younger cyber users or vice versa. The age variable was important in the study because some scholars have viewed age as an important determinant of security when using the Internet. Although the role of age on computer security is widely discussed, data examining age differences in secure technology adoption have yielded contradictory views. It is not uncommon to find scholars who argue that younger people are more confident in secure technology adoption than seniors. This notwithstanding, such arguments seem biased especially in this epoch where increasing numbers of seniors have embraced secure technology adoption thus justifying why age was included in the study (Edwards & Engelhardt, 1989).

The age variable was categorized into three age groups. 18 to 30 covered young age participants, 31 to 50 covered middle age participants, while 51 and older covered older age participants. The age variable was then compared with the concern for cybersecurity variables in SPSS to determine the nature of the relationship that exist between both variables. From the case processing summary Table 35 below, a summary of the valid, missing, and total number of cases of participation was presented. The table indicates that out of a total number of 433 participants, 432 valid cases were recorded while 1 of the cases was missing. Here is the case processing summary Table 35 below.

Table 35

Case Processing Summary Table of Age and Concern for Cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
How old are you? * Please rate your concern for security.	432	99.8%	1	0.2%	433	100.0%

Since the case processing summary table only gave an overview of the results, it was important to understand in detail what would happen when both variables are equated with each other in contingency tables. The concern for cybersecurity variable was placed in the columns while the age variable was placed in the rows of the table when running the cross-tabs in SPSS. From the below Crosstab Table 36 some high water marks were noticeable. Out of the 432 participants who responded to the question, 91.5% (118) of young age participants were highly concerned about security when using the Internet. 92.4% (171) of middle age participants were highly concerned about security when using the Internet. 94.9% (112) of older age participants were highly concerned

about security when using the Internet. No (0.0%) participant from the young age and the older age categories indicated that they had no concern for security when using the Internet. Only one (0.5%) participant from the middle age category had no concern for security when using the Internet.

What was evident from the analysis is the fact that majority of the participants irrespective of their age category were highly concerned about security when using the Internet. However, it was not possible considering the demographic employed in the study to understand what cyber users who are younger than 18 or specific cyber users like millennials or baby boomers could think about Internet security. Here is the crosstab Table 36 below.

Table 36

Contingency Table of Age and Concern for Cybersecurity

How old are you? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
How old are you?	18 - 30	Count	0	4	7	118	129
		% within Row	0.0%	3.1%	5.4%	91.5%	100.0%
		% within Column	0.0%	80.0%	28.0%	29.4%	29.9%
	31-50	Count	1	0	13	171	185
		% within Row	0.5%	0.0%	7.0%	92.4%	100.0%
		% within Column	100.0%	0.0%	52.0%	42.6%	42.8%
	51 and older	Count	0	1	5	112	118
		% within Row	0.0%	0.8%	4.2%	94.9%	100.0%
		% within Column	0.0%	20.0%	20.0%	27.9%	27.3%
Total		Count	1	5	25	401	432
		% within Row	0.2%	1.2%	5.8%	92.8%	100.0%
		% within Column	100.0%	100.0%	100.0%	100.0%	100.0%

A bar chart represented by Figure 11 below was also configured to describe the crosstab results graphically. The age variable appeared on the x-axis of the graph while the concern for security variable appeared on the y-axis of the graph. A careful look on the graph indicates that the graph substantiates the analysis presented in the crosstabs above as it is clear that majority of the participants irrespective of their age indicated that they were highly concerned about security when using the Internet. Take a look on the bar chart Figure 9 below.

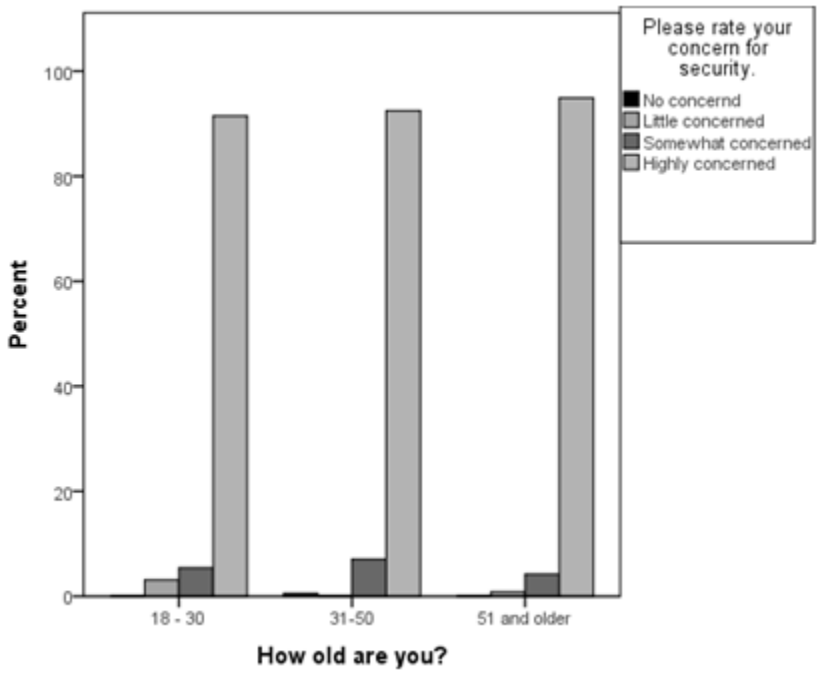

Figure 9. Age and concern for cybersecurity.

Considering the fact that the case processing summary table, the cross-tabulation table, and the bar charts did not indicate the level of statistical significance of the variables, the Pearson's Chi-square test of independence represented by Table 37 was conducted. The Chi-square results were not significant as justified by the obtained asymptotic significance p-value of .181. The relationship between age and concern for security was interpreted not to be significant because the obtained p-value of .181 was

above the stated alpha value of .05%. These results meant that the alternate hypothesis had to be rejected and the null accepted. The results also indicated that cyber users are not concerned about security because of their age. Here are the results and the Chi-square table below.

$$X^2 \ (6, N = 432) = 8.878, p = .181$$

Table 37

Pearson Chi-square Statistics of Age and Concern for Cybersecurity

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.878[a]	6	.181
Likelihood Ratio	10.070	6	.122
Linear-by-Linear Association	1.705	1	.192
N of Valid Cases	432		
a. 6 cells (50.0%) have expected count less than 5. The minimum expected count is .27.			

Cross-Tabulation of Residence Location and the Importance of Cybersecurity

Residence location was included as an independent variable in the study because of the desire to understand if a cyber users' home location contributed in determining how concerned they felt about the security of the Internet. To understand the relationship that exists between resident location and concern for security, both variables were included in the questionnaire that was presented to survey participants. Four hundred thirty-three participants took part in the study, and data was then exported from the SuveyMonkey platform to SPSS for analysis.

From the case processing summary Table 38 below, the valid, missing, and total number of cases of participants that answered the residence location question and the

concern for security question was presented. Out of the 433 people who participated in the survey, 99.3% (430) of them answered the residence location and the concern for security question while three missing cases were recorded. Here is the table below.

Table 38

Case Processing Summary Table of Residence Location and Concern for Cybersecurity

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What is your residence? * Please rate your concern for security.	430	99.3%	3	0.7%	433	100.0%

Considering the fact that the case processing summary table did not give details of the relationship that exist between residence location and concern for security, the cross-tabulation analysis was conducted in SPSS represented by Table 39 below. The concern for security variables appeared in the columns of the table while the residence location variable appeared in the rows of the table. Out of the 430 participants who answered the question, 92.8% (324) of participants resident in Urban America were highly concerned about security when using the Internet. 92.6% (75) of participants resident in Rural America were highly concerned about security when using the Internet. No (0.0%) participant who identified their residence as ‘Urban America’ indicated that they were not concerned about security when using the Internet. Only 1 (1.2%) participant resident in Rural America was not concerned about security when using the Internet.

Looking at the crosstab results it is evident that majority of participants irrespective of their place of residence were highly concerned about security when using the Internet. Participant’s level of concern for the security of the Internet was not

something that was determined by their residence location as most of the participants indicated that they were highly concerned about security when using the Internet. Here is the cross-tabulation Table 39 below.

Table 39

Contingency Table of Residence Location and Concern for Cybersecurity

What is your residence? * Please rate your concern for security.							
			Please rate your concern for security.				
			No concerned	Little concerned	Somewhat concerned	Highly concerned	Total
What is your residence?	Urban America	Count	0	3	22	324	349
		% within Row	0.0%	0.9%	6.3%	92.8%	100.0%
		% within Column	0.0%	60.0%	88.0%	81.2%	81.2%
	Rural America	Count	1	2	3	75	81
		% within Row	1.2%	2.5%	3.7%	92.6%	100.0%
		% within Column	100.0%	40.0%	12.0%	18.8%	18.8%
Total		Count	1	5	25	399	430
		% within Row	0.2%	1.2%	5.8%	92.8%	100.0%
		% within Column	100.0%	100.0%	100.0%	100.0%	100.0%

The tables above did not describe the relationship in a way that was easy to identify the important percentages quickly. To give a graphical description of the relationship which, is necessary for easy understanding, SPSS was configured to produce the bar chart Figure 10 below. The residence location variable appeared on the x-axis of the graph while the concern for security variables appeared on the y-axis of the chart. The results of the graph corroborate the analysis presented in cross-tabs by justifying that majority of participants irrespective of their residence location are highly concerned about security when using the Internet. Cyber users are not more or less concerned about Internet security just because of where they live. Here is the bar chart Figure 10 below.

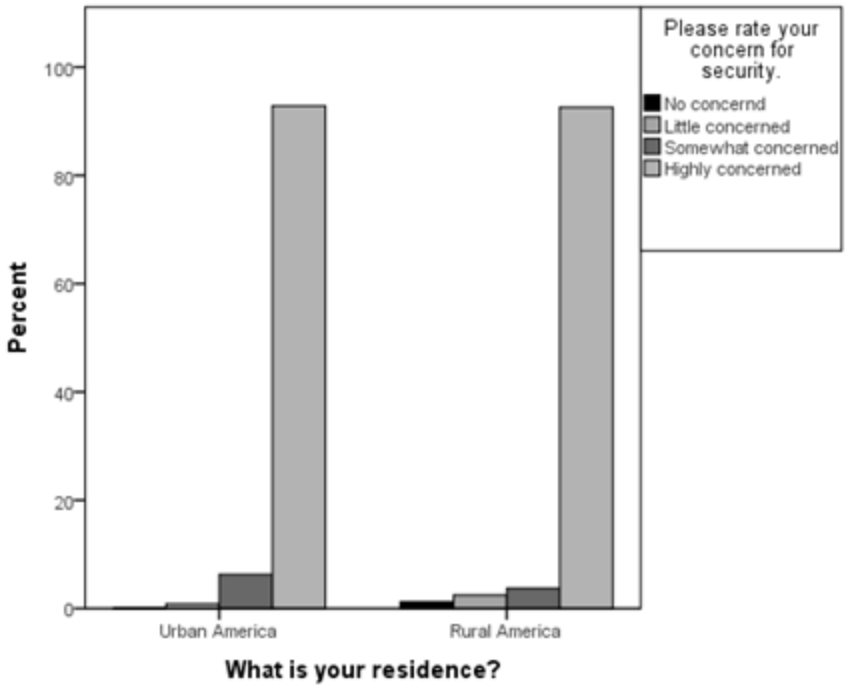

Figure 10. Residence location and concern for cybersecurity.

It is important to indicate that the above tables and graphs did not explain statistical significance between residence location and concern for security thus making it difficult to understand if the relationship was significant or not. To know the level of statistical significance of the variables, Chi-square test represented by Table 40 was conducted. The Chi-square results were not significant as justified by the .088 asymptotic significance value which, was slightly higher than the stated alpha value of .05. IT should be mentioned that the .088 significance value would have revealed evidence of a relationship if a slightly higher alpha value was established for the study. Nonetheless the .05 alpha set for the study remains and so justifies signs of no relationship between the variables. The obtained results meant that there was evidence of no relationship between a cyber user's residence location and their level of concern for security thus justifying the

rejection of the alternate hypothesis and the acceptance of the null hypothesis. Here are the results and the Chi-square table.

$$X^2 \ (3, N = 430) = 6.538, p = .088$$

Table 220

Pearson Chi-square Statistics of Residence Location and Concern for Cybersecurity

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.538[a]	3	.088
Likelihood Ratio	5.392	3	.145
Linear-by-Linear Association	1.041	1	.308
N of Valid Cases	430		
a. 5 cells (62.5%) have expected count less than 5. The minimum expected count is .19.			

Conclusion

This chapter focused on presenting the cross-tabulation of the dependent variable (concern for cybersecurity) and the independent variables with the ultimate goal of determining whether or not a relationship existed between the variables, as well as understanding statistical significance and strength of the relationship. Case processing summary tables, cross-tabulation tables, and Pearson's Chi-square test of independence, bar charts, and Lambda and Gamma tests were used to explain the relationship between the study variables. From the analysis, it was determined that training and type of business conducted on the Internet had a relationship with concern for security while the rest of the other variables did not. Whether or not evidence of a relationship was determined, all findings were important and gave unique perspectives on how participants thought about security and the independent variable in question. The independent

variables that showed evidence of a relationship with security in chi-square had low Lambda and Gamma effects indicating that the relationship was not a significant one. These obtained results did not only reveal the stance of the sample used in the study but also highlighted the fact that the sample was Internet savvy and knew the importance of Internet security for their daily Internet use. Chapter five focuses on explaining the findings and highlighting their relevance and application to theory and suggesting ways to move forward with Internet usage in a manner that is secure and respects the privacy of our valuable data assets.

Chapter 5: Discussion and Implications of the Study

Introduction

This chapter presents the findings of the research and expounds on the impact that the findings have on cybersecurity awareness and systems theory, social change, crisis management and conflict resolution practice, and information assurance in organizations. Drawing from the findings of the study; recommendations are made to guide information security professionals, IT system users, conflict resolution practitioners, business managers and policy developers on best practices to secure cyberspace use. While these recommendations are not exhaustive in themselves, they lay a solid foundation for secure Internet use and provide avenues for further research geared at promoting security in IT.

A Summary Discussion of Findings of the Hypothesis Tested

Before presenting the results, it is important to give a recap of what this study was all about as it would highlight the significance of the findings to secure cyber use. The focus of the research was to understand attitudinal differences in Internet use and security with the objective of understanding the relationships that cyber utilization have on the occurrence of cybercrime and then identify best practices needed to ensure data integrity by preventing malicious attacks within acceptable levels of cost, and risk. To achieve the objectives of the research, the following null hypotheses were tested.

Hypothesis H01: There is no significant association between the Internet users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity.

Hypothesis H02: There is no significant association between Internet users considering themselves as IT savvy and their level of concern for cybersecurity.

Hypothesis H03: There is no significant association between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity.

Hypothesis H04: There is no significant association the amount of financial loss incurred due to cyber breach and level of concern for cybersecurity.

Hypothesis H05: There is no significant association between the educational level of the cyber user and their level of concern for cybersecurity.

Hypothesis H06: There is no significant association between the gender of the cyber user and their level of concern for cybersecurity.

Hypothesis H07: There is no significant association between the age of the cyber user and their level of concern for cybersecurity.

Hypothesis H08: There is no significant association between the residence location of a cyber user and their level of concern for cybersecurity.

To test these hypotheses, a questionnaire was posted on SuveyMonkey, and 433 surveys were collected. Data was exported into SPSS, and a combination of cross-tabulation analysis, bar charts, Chi-square test of independence, Lambda and Gamma tests were employed to analyze the data. Here are the findings obtained below.

The study finding found evidence of a relationship between the cyber user's experience with cybersecurity awareness training and their level of concern for

cybersecurity. This significant relationship is justified by the obtained Chi-square statistic in Table 17 of the study. The obtained results were: X^2 (6, N=422) = 13.839, p <.031. This finding justified rejecting the first null hypothesis of the study and accepting the alternate hypothesis that favored the existence of a significant association between cybersecurity awareness training and cyber user's level of concern for cybersecurity. Nonetheless, while there was evidence of a relationship, the obtained Lambda value of .006 in Table 18 showed a weak level of association between the variables. This means that cybersecurity awareness training would have a very low ability to reduce the number of errors made from predicting the cyber use's level of concern for cybersecurity. Confer table 41 below for the summary of the results.

The study finding did not find evidence of a relationship between cyber users considering themselves as IT savvy and their level of concern for the security of the Internet. This less significant relationship is justified by the obtained Chi square statistic results found on Table 21 of the study. The obtained results were: X^2 (3, N=432) = 1.388, p = .708. This finding justified rejecting the second alternate hypothesis of the study and accepting the null hypothesis that disapproves the existence of a relationship between cyber users considering themselves as IT savvy and their level of concern for the security of the Internet. Confer table 42 below for the summary of the results.

The study finding found evidence of a relationship between the type of transaction conducted on the Internet and the cyber user's level of concern for cybersecurity. This significant association is justified by the obtained Chi-square statistic in Table 24 of the study. The obtain results were: X^2 (9, N=431) = 37.939, p <.001. This finding justified rejecting the third null hypothesis of the research and accepting the alternate hypothesis

that argued in favor of the existence of a relationship between the types of transaction conducted on the Internet and the cyber user's level of concern for cybersecurity. This notwithstanding, while there was evidence of a relationship the obtained Gamma value of p .297 in Table 25 was low to predict in confidence that the type of transaction conducted on the Internet would have a relationship with security in all cases. Confer table 41 below for the summary of the results.

The study finding did not find evidence of a relationship between the associated financial cost incurred from a cyber breach incident and the cyber user's level of concern for cybersecurity. This less significant relationship is justified by the obtained Chi-square statistic in Table 28 of the study. The obtained results were: X^2 (4, N = 392) = 2.277, p = .685. This finding justified rejecting the fourth alternate hypothesis of the study and accepting the null hypothesis that argued that there is no relationship between the associated financial cost incurred from a cyber breach and the cyber user's level of concern for cybersecurity. Confer table 42 below for the summary of the results.

The study finding did not find evidence of a relationship between the educational level of the cyber user and their level of concern for cybersecurity. This less significant relationship is justified by the obtained Chi square statistic results found on Table 31 of the study. The obtained results were: X^2 (9, N=432) = 11.016, p = .275. This finding justified rejecting the fifth alternate hypothesis of the study and accepting the null hypothesis that disapproves the existence of a relationship between the educational level of the cyber user and their level of concern for cybersecurity. Confer table 42 below for the summary of the results.

The study finding did not find evidence of a relationship between the gender type of the cyber user and their level of concern for the security of the Internet. This less significant relationship is justified by the obtained Chi-square statistic in Table 34 of the study. The obtained results were: X^2 (6, N=432) = 1.765, p =.940. This finding justified rejecting the sixth alternate hypothesis of the study and accepting the null hypothesis that argued that there is no significant association between the gender of the cyber user and their level of concern for cybersecurity. Confer table 42 below for the summary of the results.

The study finding did not find evidence of a relationship between the cyber users' age and their level of concern for Internet security. This less significant relationship is justified by the obtained Chi-square statistic in Table 37 of the study. The obtained results were: X^2 (6, N = 432) = 8.878, p = .181. This finding justified rejecting the seventh alternate hypothesis of the study and accepting the null hypothesis that argued that there is no significant relationship between the age of the cyber user and their level of concern for cybersecurity. Confer table 42 below for the summary of the results.

The study finding did not find evidence of a relationship between the place of residence of the cyber user their level of concern for Internet security. This less significant relationship is justified by the obtained Chi-square statistic in Table 40 of the study. The obtained results were: X^2 (3, N = 430) = 6.538, p = .088. This finding justified rejecting the eighth research hypothesis and accepting the null hypothesis that argued that there is no significant relationship between the place of residence of the cyber user and their level of concern for cybersecurity. Confer table 42 below for the summary of the results.

Table 41

A Table of Results That Are Significant in Chi-square but Low in Their Lambda or Gamma Effect

Hypothesis tested	**Statistical results**
H01 There is no significant association between the Internet users' attitude towards the importance of cybersecurity awareness training and their level of concern for cybersecurity.	X^2 (6, N=422) = 13.839, p <.031, λ=.006
H03 There is no significant association between the type of transaction the user mostly uses the Internet for and their level of concern for cybersecurity.	X^2 (9, N=431) = 37.939, p<.001, G=.297

Table 42

Table of Results That Were Not Statistically Significant in Chi-square

Hypothesis tested	**Statistical results**
H02 There is no significant association between Internet users considering themselves as IT savvy and their level of concern for cybersecurity.	X^2 (3, N=432) = 1.388, *p* =.708
H04 There is no significant association the amount of financial Loss incurred due to cyber breach and level of concern for cybersecurity.	X^2 (4, N = 392) = 2.277, *p* = .685
H05 There is no significant association between the educational level of the cyber user and their level of concern for cybersecurity.	X^2 (9, N=432) = 11.016, *p* = .275
H06 There is no significant association between the gender of The cyber user and their level of concern for cybersecurity.	X^2 (6, N=432) = 1.765, *p* =.940.
H07 There is no significant association between the age of the cyber user and their level of concern for cybersecurity.	X^2 (6, N = 432) = 8.878, *p* = .181
H08 There is no significant association between the residence location of a cyber user and their level of concern for cybersecurity.	X^2 (3, N = 430) = 6.538, *p* = .088

Analysis of the Results That Did Not Reveal a Relationship with Literature

While one study may explain certain findings and patterns among some variables, sampling method, size, and statistical test used in the research play a major role in determining the results of the study. This study used a sample of college/university students of all genders in the Washington, DC, area who range between the ages of 18

and older and use the Internet. This sample determined the obtained findings as the results might have looked different if other samples/tests were utilized for the study.

When the study variables that found no relationship with concern for security are compared to previously held views on cybersecurity, some differences are identified. These differences undermine statements that project relationships between those variables and security. While researchers would like to have findings that confirm their research hypotheses, differing findings are also important as they suggest new ways of thinking and orienting research.

While cybersecurity literature consistently recognizes the role that gender plays in determining how cyber users view security, this study findings have challenged those views by suggesting that the views of cyber users towards security are independent of their gender type. Consequently, the finding that there is no relationship between gender and concern for security have undermined the belief that women are less likely to be concerned about computer and Internet security than men. While these views may have been prominent decades ago, the evolution of computer science and the widespread use of computers and cyber knowledge have eroded the gender gap in secure computer adoption (Kominski, 1992; Kominski & Newburger, 1999).

The impact of the evolution of computer science and secured Internet use is the disappearance of the role of gender as a factor influencing users' attitudes towards cyber utilization. This shift in paradigm, according to some researchers, started in the early 1990s and continued ill date (Bikson & Panis, 1995; National Telecommunications and Information Administration, 2002). Today it is noticeable that women are more or less

likely to use computers than men and as a result care about secure Internet use especially for work related purposes (Bikson & Panis, 1995; Kominski & Newburger, 1999).

Some segments of cybersecurity literature uphold the idea that the age of the cyber user is a determinant variable of how the cyber users view security in IT. This view is probably explained by the fact that greater majority of those who readily embrace new technologies are most likely to be young, male, better educated, more affluent, and urban residents. Thus explaining why some scholars still contend that men would be more concerned about secured Internet adoption than women (Norris, 2001; Rogers, 1995). This notwithstanding, constant technological advancement and evolution with time have revealed the indispensable role of technological use for people of all ages.

It should also be stated that decades ago when healthcare was less advanced, it was noticeable that seniors were not as healthy as they are today, making it difficult for some to have the capability and stamina to learn and adapt to technological developments. Such a situation created the false belief that seniors are resistant to change and unwilling to interact with 'high tech' products. With the improvement in healthcare and education over time, increasing numbers of seniors are healthier and better educated, thus making it possible for them to learn and adapt to new forms of technology.

Literature also indicates that between 1970 and 2008 the percentage of seniors with high school certificates rose from 28% to 77.4% and about 20.5% of them could also boast of having a bachelor's degree or greater (Czaja et al., 2006). This improvement in literacy has impacted technology acquisition positively and has established the notion that people with higher levels of education are more likely to use technology than otherwise. Existing literature on age and information technology corroborated by the

findings of this study challenges past stereotypes and highlights the reality that people of all ages are interested in learning and using technology. Although literature shows that seniors have more computer anxiety, less computer self-efficacy, and less comfort using computers than younger adults (Czaja et al., 2006; Nair, Lee, & Czaja, 2005), they nonetheless are increasingly interested in learning and using technology securely.

Despite the recent changes explained above, literature still indicates that computer anxiety and computer self-efficacy are important predictors of secure technology adoption for people of all ages (Czaja et al., 2006; Ellis & Allaire 1999), thus making it necessary for cyber users to be knowledgeable and experienced in using technology (Adams, Stubbs, & Woods, 2005; Charness, Schumann, & Boritz, 1992; Czaja & Sharit, 2003; Dyck & Smither, 1994; Jay & Willis, 1992). These discoveries are important because by recognizing the factors that either hinder or promote secure technology adoption and understanding their origins, avenues are opened for policymakers to reassess the successes of resource allocation initiatives and as a result help redirect assets to areas where the digital divide is still wide.

Another variable that failed to realize a relationship with information security adoption was the cyber users' resident location. The cyber users' place of residence was included in the study design to explain the validity of the perspective that people who live in urban areas are more likely to use the Internet securely than people who live in the rural areas of the country given that accessibility to wireless broadband Internet is more available to urban dwellers than rural dwellers. The study found that the cyber users' place of residence does not determine the cyber user's level of concern for security.

In the same light, the study finding indicated that the associated amount of financial loss suffered from a cyber-attack is not a determining factor for secure Internet use. This finding challenged the popularly held views that cyber user's cares more about the security of the Internet especially when they lose more money from a cyber-attack. Drawing from the findings, it is important to say that the reason companies invest in cybersecurity is to ensure data availability, confidentiality, and integrity, thus explaining why literature indicates that security breaches affect organizations negatively. While cyber-attacks create a lot of problems to companies and damage customer and investor confidence all its negative outcomes amount to some form of financial loss, thus justifying why cyber users and organizations care about security irrespective of the amount of money lost.

Although cyber-attacks occur often, breaking news reports mostly cover those that involve massive amounts of financial losses. This phenomenon, unfortunately, feeds on the false narrative that concern for security is determined by the sum of money lost. The findings of this study have debunk this false narrative by indicating that concern for security does not depend on the amount of money lost for even an individual cyber user who loses $1.00 as a result of a sales scam genuinely cares about security to the same degree that a corporate CEO whose company suffers millions of dollars in financial losses as a consequence of a major cyber breach cares about security.

The study findings have also indicated that cyber users do not automatically care about the security of the Internet simply because they are IT savvy. This finding is important because it clarifies the idea that people who are knowledgeable in computers are better stewards of secure computer use. This study findings have debunk such an idea

by indicating that being IT savvy is not a prerequisite to using the Internet securely for any Internet user cares about the security of their assets irrespective of whether they are IT savvy or not.

The study finding also indicated that cyber users are not automatic stewards of secure computer adoption simply because they are educated. Education is an important function of life but at the same time education cannot predict or determine how people would behave when using the Internet. Although a structured security education program is designed to help reduce the number of security breaches that occur due to lack of security awareness (Whitman & Mattord, 2004), education in itself does not automatically ensure that people would use computers securely or care about security when using computers. Education ensures that cyber users are given the tools needed to use technology securely (Schou & Trimmer, 2004) but education cannot condition a cyber user to act a certain way as human action is determined by freewill. The findings of the study in this regard highlights the fact that people have freewill and therefore would do what they want irrespective of their educational background. Although education imparts people with the knowledge they need to make positive choices in life, it does not unfortunately condition people to behave in certain ways.

Analysis of the Results that had a Weak Relationship with Literature

It is important to begin this section by stating that while the study findings identified relationships between cybersecurity, training and the associated amount of financial loss obtained from a cyber-attack, the revealed Lambda and Gamma effects were low, thus cautioning that such results be carefully interpreted to avoid the projection of relationships that are weak in significance. A key point to make here is that those

obtained weak Lambda and Gamma values show that the independent variables of the study had a very low ability to reduce the number of errors in predicting the categories of the dependent variable. Such occurrences are not by chance but rather reflect the stance of the sample used in the study.

The Lambda and Gamma effect obtained from comparing the variables does not only reflect the type of sample used in the study, but most importantly the sample's prior knowledge of security and its effect on cyber utilization. Therefore, to make sense of the results and interpret them correctly, the samples prior knowledge of security must be fully understood so as to interpret the obtained Chi-square, Lambda, and Gamma values correctly. The obtained weak Lambda and Gamma values have some connection to the obtained low chi-square cell counts which, are also connected to the stance of the sample used in the study. All these queries stem from the fact that majority of the study participants automatically favored secure Internet adoption because most of them had already taken security training and therefore already knew the damaging effects of a cyber-attack. As a result most of their responses were directed towards the categories that favored security thus recording low numbers on the categories that did not favor security.

The observation at this point of the study which, has been partly discussed in chapter four is that university students in the Washington, DC, area and their prior knowledge and preference for cybersecurity and security awareness training placed them in one category and tailored their responses to lean more in favor security in IT. This, therefore, created a situation where cell groups that were not in favor of security were either empty or had low data, thus making it impossible to find strong Lambda or Gamma values.

Nonetheless, these obtained weak Lambda or Gamma values are essential for research because they create an opportunity for future scholars to test the relationship between the variables using different samples like millennial, baby boomers, or uneducated cyber users to compare and see if the results would reveal something new. The cyber threat problem is a very critical issue in the 21st century, and any opportunity to expand cybersecurity research should be embraced by scholars, and that is a significant contribution of this study to scholarship.

The existence of a weak association between cybersecurity awareness training and concern for security is not only an important indicator of the important role that cybersecurity training plays on secure computer adoption, but also explains why almost all study participants have taken some form of cybersecurity training and feel that training is important and necessary, thus making it impossible to find a statistically significant relationship between cybersecurity training and security.

Although the obtained Lambda value of .006 reveals a weak relationship, it is nonetheless important as it discloses the fact that the study sample already knows the importance of cybersecurity training and have embraced it as a continuous function of their cyber use attitude even if their experience cannot be extended to other populations. To benefit from such a situation, further research on the same topic could be conducted using different samples to compare and see if the values are different.

The identified Chi-square significance between the type of Internet transaction and concern for security highlights the importance of security for all Internet transactions despite the Gamma value of p .297. An important function of the obtained Gamma value here is the fact that the results are only relevant to the sample used in the study. While

this study centered on finding out relationships among variables, also knowing the strength of association is important as it prevents overly projecting statistically insignificant relationships. Although the Gamma value of p .297 was low and had some connection to the obtained low chi-square cell counts, the value nonetheless justified expanding research by using different samples or testing different variables which, is an important discovery of this study.

It is important to indicate that although all Internet transactions demand security, some transactions are more sensitive than others, thus compelling higher levels of clearance and permissions for personnel whose jobs require access to those operations. The sensitivity of some operations highlights the concept of creating layers of security which, in itself creates the necessity to segment security on a 'need-to-know' basis so that cyber users can only access what they are authorized to access. Security segmentation does not jeopardize security but rather limits the damage that could be caused to an environment if a disgruntled insider or hackers for that matter were to cause harm to a system. Careful observation of 'need-to-know' is what helps limit the possible damage that could be caused.

Conclusion and Implication of the Findings

Implication of the findings vis-à-vis systems theory and holistic cybersecurity awareness

One fundamental lesson drawn from the study findings is the indication from research participants that Internet security is an essential element of the cyber usability. This revealing statement from all crosstabs solidifies the necessity for all cyber users and business owners to build an efficient and systematic cybersecurity platform that ensures

secure business operations. Such an efficient approach to security would validate the implementation of a systems theory culture that would ensure that all cyber stakeholders are in alignment with the business of maintaining security in IT since one bad player in the cybersecurity venture jeopardizes the efforts of all.

The proposal of a systems theory approach to security is backed by the overwhelming crosstab results that indicate the fact that, despite a cyber user's age, gender, educational level, being IT savvy, residence location, associated amount of financial loss from a cyber-attack, majority of study participants feel that Internet security is a fundamental element of their Internet usability. Therefore, incorporating a systems theory approach to cybersecurity utilization would ensure that no matter a cyber user's situation, all the necessary resources would be employed to build an effective cybersecurity infrastructure and one fundamental remedy to the cyber-threat problem is cybersecurity awareness training.

Literature also recommends a systems theory approach to information security because the foundation of systems theory is the evolution of systems and the interdependence that creates unity and shared purpose for all system components (Moeller & Valentinov, 2012; von Bertalanffy, Juarrero, & Rubino, 2008). This is important because dysfunctional systems nurse future cybersecurity problems (Coole & Brooks, 2014).

Adopting a systems theory approach to the impending cyber-threat problem would be a real enhancement to the cybersecurity awareness effort because through it cybersecurity awareness training programs will cease focusing solely on content and

process but also on how cyber users approach cybersecurity decision-making, thus enhancing cybersecurity in a holistic fashion (Tsohoua, Karydab, & Kokolakis, 2015).

The implementation of a diverse cybersecurity awareness training program influenced by a systems theory philosophy will ensure successful IT operations in organizations by deploying a comprehensive approach to employee training (Chandrashekhar, Gupta, & Shivaraj, 2015), thus creating a workforce that understands cybersecurity and its implications to business.

Also, the application of a systems theory approach to cybersecurity awareness training will create a cybersecurity culture in the entire organization by establishing the need for security principles to be applied to all sectors of the company. This approach will help incorporate security compliance into employees' work ethic and assists cyber users with developing attitudes that are in line with effective security policies and procedures (Parsons et al., 2015).

A systems theory approach to security will also highlight the overwhelming indication from study participants that no matter a cyber users' situation, Internet security is an important function of IT use and should be enforced insure data confidentiality, integrity and availability. This observation would drive business leaders to design cybersecurity awareness training programs that are holistic, eclectic, robust, and cater for the security needs of the entire system.

Implication of findings vis-à-vis best practice and social change

Best practice is a process that has been tested and proven successful and is accepted to be superlative when compared to other methods, thus making it a standard way of operating in an IT environment. Best practice is important in information security

because it ensures data availability, integrity, and confidentiality of business assets. A systems theory best practice approach to security would, therefore, ensure that all the components of a system are operating in unison for increased and secured business performance. This will in effect guarantee the reduction of the technical and non-technical cost associated with responding to cyber-attacks.

Implementing best practice for social change in an IT environment is encouraged because approximately 81% of the cyber-attacks result in the theft of consumer data (Lai, Li, & Hsieh, 2012), and these attacks damage the reputation of the company (Chen, Ramamurthy, & Wen, 2015). Since the majority of the study participants indicated in contingency tables that Internet security was an important factor of their Internet usability, the engine that propels security then is best practice which, is achieved by applying both the technical and non-technical components of IT.

For best practice to flourish in a cyber environment, all the stakeholders must set strong, enduring examples for every cyber user to emulate. When this is done, a conscious security culture is established in the environment which, in turn, limits cyber-attacks which, according to Hille, Walsh, and Cleveland (2015), affected more than 4% of the United States population in 2012 costing $12 billion.

Worthy of mention here is the fact that professional practice is tied to best practice in this final stage of the study. Therefore, to maintain security in an IT environment, cyber users should implement professional practice to reduce the gap that exists between technology adoption and security as security strategies and technology adoptions have consequences on an organization’s data privacy, and security awareness initiatives (Herath et al., 2014).

Implementing best practice is much needed because new technology is always being introduced into an IT environment because of constant innovation to meet the changing requirements of the time (Atienza et al., 2015). Some of these new pieces of technology help close technical loopholes and also ease technology use, thus mitigating security risk (Min, Lim, & Park, 2015).

Organizations that adopt best practice as a business philosophy build a culture of deterrence and security needed for efficient business operation and client trust (Ahmad, Maynard, & Park, 2014). This best practice culture makes security a natural aspect of cyber users' attitudes and builds confidence among business and clients (Alnatheer, 2014)

Implications of findings vis-à-vis crisis management and conflict resolution

As already stated above the underlining objective that guides cybersecurity and risk management frameworks are the desire to guarantee the confidentiality, integrity, and availability of data assets which, are constantly under attack from cyber criminals. Since hacking has been identified as a serious problem in IT, the assistant direction of the FBI Gordon Snow, is correct when he cautions all cyber users to get prepared to be hacked (Gordon Snow, 2011). Cyber users should take Gordon's statement positively for in preparing to be hacked they are in effect covering the vulnerabilities that could be exploited by hackers. If Gordon's exultation is taken seriously, cyber users will approach cybersecurity from a risk management mindset. This mindset will ensure that systems are monitored, and vulnerabilities are remediated before they are exploited by hackers.

The reality is that frequent cyber-attacks on company networks have instigated many response paths, some of which, have led to congressional hearings (Bailey, 1984).

Though some companies have responded to these attacks in ways that leave their infrastructure unscathed, others have reacted in a manner that opens doors to further criticism. Most often than not, the outcome of these cyber-attacks not only depends on the damage caused but also on the organization's ability to demonstrate a structured and orderly handling of the incident. This notwithstanding, cyber-attacks are wrong and cause massive and costly lawsuits that are damaging to the reputation of the organization. From a conflict resolution perspective, a proposed solution to the cyber risk problem is a risk management approach to cybersecurity.

Recommendations for Action and the Way Forward

Taking into consideration the overwhelming indication by researcher participants that Internet security is an important function of IT usability, the fortification and building of cyber defense systems to protect IT assets from internal and external threats is critical to IT use and the success of any business operation (Carter et al., 2012). Therefore, cyber users and stakeholders should relentlessly search for best practices needed to secure IT systems and protect data from costly cyber-attacks (Caldwell, 2012).

Guided by both the study findings and best practice, the following recommendations are presented as guides to building a robust cybersecurity program embedded in theory and practice.

a. The need to implement mandatory cybersecurity awareness training programs to mitigate cyber-attacks. This recommendation is justified by the finding in support of the first research hypothesis that argues in favor of a relationship between cybersecurity awareness training and concern for Internet security. Cybersecurity

awareness training is essential because it teaches cyber users to understand and fully appreciate their role in maintaining a cyber safe work environment.

b. The necessity to conduct research on a similar topic using different samples like millennials, baby boomers, and uneducated cyber users to compared the results of both studies and learn from what might change. This recommendation would not only explain the identified Chi-square low cell count queries but would also explain the weak Lambda and Gamma values that made the relationship insignificant.

c. The necessity for cyber users and organizations to share best practices needed for an efficient system theory approach to security. This finding is supported by the revealed relationship between cybersecurity awareness training and concern for security. The strength obtained from participating in a cybersecurity awareness training program emerges from best practices that have been tested and proven to be successful in upholding security in an IT environment.

d. The need to implement a risk management and governance approach to cybersecurity practice. This recommendation is important because it highlights the reality of the unavoidable risks that exist in IT and advocates the need to evaluate, identify, and assess risk and possibly eradicate the potential internal and external attacks that threaten the smooth functioning of IT.

e. The necessity to establish a continuous monitoring program that helps identify and stop hacks by engaging in what could be called ‘cyber mediation’ or ‘cyber diplomacy’. This proposal is crafted from the idea that just as DHS develops software to apprehend illegal immigrants crossing the southern border, software

could equally be develop and used to engage cyber intruders in real time thus neutralizing the harm such a hack could cause.

To conclude, many scholars have argued that the immersion of research findings in training manuals, policy documents, and academic literature builds theory and provides new insights of thinking (Aydm, 2012). For that reason, publishing and disseminating research findings to a wider audience is an important function of research (Saracho, 2013). The hope is that this research should present a window of opportunity to all cyber users to cherish and promote the secure use of IT systems which, are constantly being attacked by hackers.

References

Abraham, S. (2011). Information security behavior: Factors and research directions. AMCIS 2011 Proceedings - All Submissions. Paper 462.

Achebe, C. (1958). *Things fall apart*. Oxford, UK: Heinemann Educational Publishers.

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study*. Twenty Seventh International Conference on Information Systems (ICIS), Milwaukee, WI. Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46. http://dx.doi.org/10.1145/322796.322806

Adams, N., Stubbs, D., & Woods, V. (2005). Psychological barriers to Internet usage among older adults in the UK. *Medical Informatics and the Internet in Medicine, 30*(1), 3.

Adebayo, A. O. (2012). A foundation for breach data analysis. *Journal of Information Engineering and Applications, 2*(4), 17-23. Retrieved from http://www.iiste.org/Journals/index.php/JIEA

Agresti, A. (1990). Categorical data analysis (2nd ed.). New York: John Wiley & Sons, Inc.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*, 357-370. doi:10.1007/s10845-012-0683-0

Aitoro, J. R. (2010, August 19). Roles and responsibilities key to making cybersecurity work. *NextGov.* Retrieved from http://www.nextgov.com/cybersecurity/2010/08/roles-and-responsibilities-key-to-making-cybersecurity-work/47423/

Ajzen, I. (1988). *Attitudes, personality, and behavior.* Homewood, IL: Dorsey Press.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Akers, R. L. (2000). *Criminological theories: Introduction, evaluation, and application* (3rd ed.). Los Angeles: Roxbury Publishing Company.

Aldesco, A. I. (2002). The demise of anonymity: A constitutional challenge to the convention on cybercrime. *Loyola of Los Angeles Entertainment Law Review, 23*(1), 81-123. Available from http://digitalcommons.lmu.edu/elr/vol23/iss1/3

Alexiades, M. N. (Ed.). (1996). *Selected guidelines for ethnobotanical research: A field manual*. Bronx, NY: New York Botanical Garden.

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity, 4*, 104-107. doi:10.7763/IJSSH.2014.V4.327

American Psychological Association. (2006). *Answers to your questions about transgender individuals and gender identity*. Retrieved from http://www.lgbt.ucla.edu/documents/APAGenderIdentity.pdf

Andrews, D. (1983). The legal challenge posed by the new technology. *Jurismetrics, 24*(1), 43-57. http://www.jstor.org/stable/29761847

Araque, J. C., Maiden, R. P., Bravo, N., Estrada, I., Evans, R., Hubchik, K.,…Reddy, M. (2013). Computer usage and access in low-income urban communities. *Computers in Human Behavior, 29*(4), 1393-1401. http://dx.doi.org/10.1016/j.chb.2013.01.032

Arch, E. C., & Commins, D. E. (1989). Structured and unstructured exposure to computers: Sex differences in attitudes and use among college students. *Sex Roles, 20*(5), 245-255. doi:10.1007/BF00287722

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cybersecurityfor people and organizations. *Journal of Library Administration, 54*(1), 46-56. doi:10.1080/01930826.2014.893116

Atienza, A. A., Zarcadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W. Y. S., & Pritts, J. (2015). Consumer attitudes and perceptions on health privacy and security: Findings from a mixed-methods study. *Journal of Health Communication, 20,* 673-679. doi:10.1080/10810730.2015.1018560

Aydın, O. T. (2012). The impact of motivation and hygiene factors on research performance: An empirical study from a Turkish university. *International Review of Management and Marketing, 2*, 106-111. Retrieved from http://www .ilhanozturk.com/index.php/irmm/index

Bailey, D. (1984). Attacks on computers: Congressional hearings and pending legislation. *Security and Privacy,* 180-186. doi:10.1109/SP.1984.10012

Baker, T. L. (1994). *Doing social research* (2nd ed.). New York: McGraw-Hill, Inc.

Bansal, P., & Corley, K. G. (2011). The coming of age for qualitative research: Embracing the diversity of qualitative methods. *Academy of Management Journal, 54*(2), 233-237.

Barrett, N. (1997). *Digital crime: Policing the cybernation*. London: Kogan Page.

Bell, S. (1996). *Learning with information systems: Learning cycles in information systems development.* New York: Routledge.

Bennett, C. (2014, October 14). Study: Cyberattacks up 48 percent in 2014. *The Hill.* Retrieved from http://thehill.com/policy/cybersecurity/221936-study-cyber-attacks-up-48-percent-in-2014

Bernard, H. R. (2002). *Research Methods in Anthropology: Qualitative and quantitative methods* (3rd ed.). Walnut Creek, CA: AltaMira Press.

Bernard, H. R., Pelto, J. P., Werner, O., Boster, J., Romney, A. K., Johnson, A.,… Kasakoff, A. (1986). The construction of primary data in cultural anthropology. *Current Anthropology*, *27*(4), 382-396. doi:10.1086/203456

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, *23*(3), 253-264. http://dx.doi.org/10.1016/j.cose.2003.09.002

Bigelow, R. P. (1985). The challenge of computer law. *Western England Law Review, 7*(3), 397-404.

Bikson, T. K., & Panis, C. W. A. (1995). Computers and connectivity: Current trends. In R. H. Anderson, T. K. Bikson, S. A. Law, & B. M. Mitchell (Eds.), *Universal access to e-mail: Feasibility and societal implications* (pp. 13-40). Santa Monica, CA: RAND.

Bimber, B. (2000). Measuring the gender gap on the Internet. *Social Science Quarterly, 81*(3), 868-876.

Bishop, M. (2000). Education in information security. *IEEE Concurrency, 8*(4), 4-8.

Bishop, M. (2002). *Computer security: Art and science*. Boston: Addison-Wesley.

Bisong, A., & Rahman, M. S. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications, 3*(1), 30-45. doi:10.5121/ijnsa.2011.3103

Blackburn, R. (1993). *The psychology of criminal conduct: Theory, research, and practice*. Toronto: John Wiley & Sons.

BloomBecker, J. (1981). The trial of computer crime**.** *Jurimetrics, 21*(4), 421-435. http://www.jstor.org/stable/29761764

Bobbitt, L. M., & Dabholkar, P. A. (2001). Integrating attitudinal theories to understand and predict use of technology-based self-service: The Internet as an illustration. *International Journal of Service Industry Management, 12*(5), 423-450. http://dx.doi.org/10.1108/EUM0000000006092

Bostrom, R. P., & Heinen, J. A. (1977). MIS Problems and failures: A socio-technical perspective. *MIS Quarterly, 1*(3), 17-32. doi:10.2307/248710

Bottom, N. R. (2000). The human face of information loss. *Security Management, 44*(6), 13-17.

Brenner, S. W. (2004). U.S. cybercrime law: Defining Offences. *Information Systems Frontiers, 6*(2), 115-132.

Broadhurst, R. (2006). Development in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(3), 408-433. http://dx.doi.org/10.1108/13639510610684674

Brodie, C. (2008). *The importance of security awareness training*. Fredericksburg, VA: SANS Institute.

Burstein, A. (2003). A survey of cybercrime in the United States. *Berkeley Technology Law Journal, 18*(1), 313-338. http://www.jstor.org/stable/24120520

Cairncross, I. (1997). *The death of distance: how the communications revolution will change our lives.* Cambridge, MA: Harvard Business School Press.

Caldwell, T., (2012). Reporting data breaches. *Computer Fraud & Security, 2012*(7), 5-10.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., & Mickunas, M. D. (2003). Towards security and privacy for pervasive computing in theories and systems. In M. Okada, B. C. Price, A. Scedrov, H. Tokuda, & A. Yonezawa (Eds.), *Software security—Theories and systems* (pp. 1-15). Berlin: Springer-Verlag.

Caniëls, M. C., Lenaerts, H. K. L., & Gelderman, C. J. (2015). Explaining the Internet usage of SMEs: The impact of market orientation, behavioural norms, motivation and technology acceptance. *Internet Research, 25*(3), 358-377. doi:10.1108/IntR-12-2013-0266

Carter, D. L. (1995). Computer crime categories: How techno-criminals operate. *FBI Law Enforcement Bulletin, 64*(7), 21-27.

Carter, L. D., Phillips, B., & Millington, P. (2012). The impact of information technology Internal Controls on Firm Performance. *Journal of Organizational and End User Computing, 24*(2), 39-49. http://dx.doi.org/10.4018/joeuc.2012040103

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004a). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92. http://dx.doi.org/10.1145/1005817.1005828

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Cegielski, C. G. (2008). Toward the development of an interdisciplinary information assurance curriculum: Knowledge domains and skill sets required of information assurance professionals. *Decision Sciences Journal of Innovative Education, 6*(1), 29-49. doi:10.1111/j.1540-4609.2007.00156.x

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229-251. http://dx.doi.org/10.1006/ijsl.1996.0015

Chandrashekhar, A. M., Gupta, R. K., & Shivaraj, H. P. (2015). Role of information security awareness in success of an organization. *International Journal of Research, 2*(6), 15-22. Retrieved from http://internationaljournalofresearch.org/

Charness, N., Schumann, C. E., & Boritz, G. M. (1992). Training older adults in word processing: Effects of age, training technique, and computer anxiety. *International Journal of Technology and Aging, 5*(1), 79-106.

Charney, S. (1994). Computer crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace. *Federal Bar News, 41*(7), 489-494.

Chaula, J. A. (2006). *A socio-technical analysis of information systems security assurance: A case study for effective assurance* (Doctoral dissertation). Stockholm University, Stockholm.

Chen, M. (1986). Gender and computers: The beneficial effects of experience on attitudes. *Journal of Educational Computing Research, 2*(3), 265-282. doi:10.2190/WDRY-9K0F-VCP6-JCCD

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems, 55*(3), 11-19. Retrieved from http://www.iacis.org/jcis/jcis.php

Clarke, M. R. (2011). *The role of self-efficacy in computer security behavior: Developing the construct of computer security self-efficacy* (Doctoral dissertation). Retrieved from http://nsuworks.nova.edu/gscis_etd/121/

Cochran, W. G. (1954). Some methods of strengthening the common Chi-square tests. *Biometrics, 10*(4), 417-451. http://www.jstor.org/stable/3001616

Collis, B. A., Kass, H., & Kieren, T. E. (1989). National trends in computer use among Canadian secondary school students: Implications for cross-cultural analyses. *Journal of Research on Computing in Education, 22*(1), 77-89. http://dx.doi.org/10.1080/08886504.1989.10781904

Coleman, P. T. (2011). The five percent: Finding solutions to (seemingly) impossible conflicts. New York City, NY: Public Affairs, Perseus Books.

Conover, W. J. (1999). *Practical nonparametric statistics* (3rd ed.). New York: John Wiley & Sons, Inc.

Coole, M., & Brooks, D. J. (2014). Do security systems fail because of entropy? *Journal of Physical Security, 7*(2), 50-76. Available from http://ro.ecu.edu.au/ecuworkspost2013/624/

Cresswell, A., & Hassan, S. (2007). Organizational impacts of cybersecurityprovisions: A sociotechnical framework. In *Social Sciences, 40th Hawaii International Conference on Systems Sciences* (p. 98). doi:10.1109/HICSS.2007.418

Creswell, J. W. (1994). *Research design: Qualitative and quantitative approaches*. Thousand Oaks, CA: Sage.

CSO Staff. (2004, November 1). Bruce Schneier: The people paradigm. Retrieved from http://www.csoonline.com/article/219787/bruce-schneier-the-people-paradigm

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychology and Aging, 21*(12), 333-352. https://dx.doi.org/10.1037%2F0882-7974.21.2.333

Czaja, S. J., Guerrier, J. H., Nair, S. N., & Landauer, T. (1993). Computer communication as an aid to independence for older adults. *Behavior and Information Technology, 12*(4), 197-207. http://dx.doi.org/10.1080/01449299308924382

Czaja, S. J., & Sharit, J. (2003). Practically relevant research: Capturing real world tasks, environments, and outcomes. *The Gerontologist, 43*, 9-18. doi:10.1093/geront/43.suppl_1.9

Czaja, S. J., & Shark, J. (1998). Age differences in attitudes toward computers. *Journal of Gerontology Psychological Sciences, 53*(5), 329-340.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339. http://www.jstor.org/stable/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003. http://dx.doi.org/10.1287/mnsc.35.8.982

De Vaus, D. A. (1996). *Surveys in social research* (4th ed.). London: UCL Press.

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research, 6*(2), 80-88. doi:10.1177/1558689812437186

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security, 20*(2), 165-172. http://dx.doi.org/10.1016/S0167-4048(01)00209-7

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128. http://dx.doi.org/10.1145/341852.341877

Dhillon, G., & Torkzadeh, R. (2006). Value-focused assessment of information systems security in organizations. *Information Systems Journal, 16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x

Diener-West, M. (2008). *Use of the chi-square statistics*. Baltimore, MD: Johns Hopkins Bloomberg School of Public Health. Retrieved from http://ocw.jhsph.edu/courses/fundepiii/pdfs/lecture17.pdf

Dizard, W. (1997). *MegaNet: How the global communications network will connect everyone on earth*. Boulder, CO: Westview Press.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security, 26*(1), 73-80.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers and Security, 25*(1), 55-63. http://dx.doi.org/10.1016/j.cose.2005.09.009

Downs, D. M., Ademaj, I., & Schuck, A. M. (2009, January). Internet security: Who is leaving the 'virtual door' open and why? *First Moday, 14*(1-5). Retrieved from http://firstmonday.org/article/view/2251/2067

Durgin, M. (2007, September). Understanding the importance of and implementing internal security measures. Available from https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php

Dyck, J. L., & Smither, J. A. (1994). Age differences in computer anxiety: The role of computer experience, gender and education. *Journal of Educational Computing Research, 10*(3), 239-248.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Orlando, FL: Harcourt Brace Jovanovich College Publishers.

Edwards, R., & Engelhardt, K. G. (1989). Microprocessor-based innovations and older individuals: AARP survey results and their implications for service robotics. *International Journal of Technology and Aging, 2*, 56-76.

Ellis, R. D., & ,Allaire J. (1999). Modeling computer interest in older adults: The role of age, education, computer knowledge, and computer anxiety. *Human Factors,* 41(3), 345-355. doi:10.1518/001872099779610996

Eloff, M. M., & von Solms, S. H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers and Security, 19*(3), 698-709. http://dx.doi.org/10.1016/S0167-4048(00)08019-6

Emery, F. E., & Trist, E. L. (1960). Sociotechnical systems. In C. W. Chruchman & M. Verhulst (Eds.), *Management sciences: Models and techniques* (Vol. 2., pp. 83-97). New York: Pergamon Press.

Eminağaoğlu, M., Ucar, E., & Eren, S. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Technical Report, 14*(4), 223-229. http://dx.doi.org/10.1016/j.istr.2010.05.002

Etzioni, A. (1997). Communities: Virtual vs. real. *Science, 277*(5324), 295.

Executive Office of the President of the United States. (2013). *Fiscal year 2012 report to congress on the implementation of the federal information security management act of 2002*. Retrieved from http://www.whitehouse.gov/sites.default/files/omb/assets/egov_docs/fy12-fisma/pdf

Federal Bureau of Investigation. (2015, January 13). FBI warns of fictitious ‘work-from-home’ scam targeting university students [Alert no. I-011315a-PSA]. Retrieved from https://www.ic3.gov/media/2015/150113-1.aspx

Feldman, M. P. (1993). *The psychology of crime a social science textbook*. Cambridge: Cambridge University Press.

Felson, M. (1994). *Crime and everyday life: Insight and implications for society*. Thousand Oaks, CA: Pine Forge Press.

Ferguson, M. J., & Bargh, J. A. (2007). Beyond the attitude object: Implicit attitudes spring from object-cantered contexts. In B. Wittenbrink & N. Schwarz (Eds.), *Implicit measures of attitudes* (pp. 216–246). New York: Guilford Press.

Fetler, M. (1985). Sex difference on the California statewide assessment of computer literacy. *Sex Roles, 13*(3), 181-191. doi:10.1007/BF00287909

Fink, A., & Kosekoff, J. B. (1985). *How to conduct surveys: A step-by-step guide*. Beverly Hills, CA: Sage.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Fishkin, J. (1992). *The dialogue of justice: Toward a self-reflective society*. New Haven, CT: Yale University Press.

Flowerday, S., & von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers and Security, 24*(8), 604-613. http://dx.doi.org/10.1016/j.cose.2005.08.004

Fontes, E. L. G., & Antonio Jose Balloni, A. J. (2007). Security in information systems: Sociotechnical aspects. In T. M. Sobh (Ed.), *Innovations and advanced techniques in computer and information sciences and engineering* (pp. 163-167). Dordrecht, Netherlands: Springer. doi:10.1007/978-1-4020-6268-1_30

Fortson, B. L., Scotti, J. R., Chen, Y., Malone, J., & Del Ben, K. S. (2007). Internet use, abuse, and dependence among students at a Southeastern regional university. *Journal of American College Health, 56*(2), 137-144. doi:10.3200/JACH.56.2.137-146

Francis, L. J. (1994). The relationship between computer related attitudes and gender stereotyping of computer use. *Computers and Education, 22*(4), 283-289. http://dx.doi.org/10.1016/0360-1315(94)90050-7

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security – A survey and classification of the research area. *Computers & Security, 30*(8), 748-769. doi:10.1016/j.cose.2011.08.002

Furnell, S. (2007). Making security usable: Are things improving? *Computers and Security*, *26*(6), 434-443.

Gainor, K. A. (2000). Including transgender issues in lesbian, gay, and bisexual psychology: Implications for clinical practice and training. In B. Greene & G. L. Croom (Eds.), *Education, research, and practice in lesbian, gay, bisexual, and transgendered psychology: A resource manual* (pp. 131-160). Thousand Oaks, CA: Sage.

Garland, K. J., & Noyes, J. M. (2005). Attitudes and confidence towards computers and books as learning tools: across-sectional study of student cohorts. *British Journal of Educational Technology, 36,* 85-91.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security, 19*(4), 216-230. http://dx.doi.org/10.1108/09685221111173049

Gattiker, U., & Kelley, H. (1997). *Techno-crime and terror against tomorrow's organization: What about cyberpunks?* Retreived from http://www.egov.ufsc.br/portal/sites/default/files/anexos/29419-29437-1-PB.html

Gercke, M. (2006). The slow wake of a global approach against cybercrime. *Computer Law Review International,* 5, 140-145.

Gercke, M. (2008). National, regional and international approaches in the fight against cybercrime. *Computer Law Review International, 9*(1), 7-13.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Goldstein, N. J., Cialdini, R. B., & Griskevicius, V. (2008, August). A room with a viewpoint: Using social norms to motivate environmental conservation in hotels. *Journal of Consumer Research, 35*. doi:10.1086/586910

Goodell, J. (1996). *The cyber thief and the Samurai*. New York: Dell Publishing.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *CSI/FBI computer crime and security survey*. Retrieved from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Grant, L. G., & Royle, T. M. (2011). Information technology and its role in creating sustainable competitive advantage. *Journal of International Management Studies, 6*(1), 1-7. Available from http://www.jimsjournal.org/pi.html

Groves, R. M., Fowler, F. J., Jr., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau. (2009). *Survey methodology* (2nd ed.). Hoboken, NJ: John Wiley and Sons, Inc.

Gupta, M., & Sharman, R. (2008). *Handbook of research on social and organizational liabilities in information security.* New York: State University of New York Press.

Hafner, K. & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.

Haley, C. B., Laney, R. C., Moffett, J. D., & Nuseibeh, B. (2006). Using trust assumptions with security requirements. *Requirements Engineering, 11*(2), 138-151. doi:10.1007/s00766-005-0023-4

Hammond, D. (2010). *Science of synthesis: Exploring the social implications of general systems theory*. Boulder, CO: University Press of Colorado.

Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social Science Quarterly, 87*(2), 432-448.

Harris, S. (2010, July 20). War of words. *NextGov*. Retrieved from http://www.nextgov.com/nextgov/ng_20100730_1013.php

Harris, S. (2013). CISSP all-in-one exam guide (6th ed.). New York: McGraw-Hill Education.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*, 61-84. doi:10.1111/j.1365-2575.2012.00420.x

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19. doi:10.1016/j.intmar.2014.10.001

Hollin, C. R. (1989). *Psychology and crime: An introduction to criminological psychology*. New York: Routledge.

Horrigan, J. B. (2010, February). *Broadband adoption and use in America* (OBI working paper series no. 1) Retrieved from https://transition.fcc.gov/national-broadband-plan/broadband-adoption-in-america-paper.pdf

Howard, J. (1997). Analysis of security incidents on the Internet (Unpublished doctoral dissertation). Carnegie Mellon University, Pennsylvania.

Hutchison, S. (1997). *Computer crime in Canada*. Unpublished manuscript.

Internet Crime Complaint Center [ICCC]. (2011). *2010 annual Internet crime report*. Retrieved from http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Isaac, S., & Michael, W. B. (1997). *Handbook in research and evaluation: A collection of principles, methods and strategies useful in the planning, design and evaluation of studies in education and the behavioral sciences* (3rd ed.). San Diego: Educations and Industrial Testing Services.

ITU. (2012, September). *Understanding cybercrime: Phenomena, challenges and legal response* (Prepared by Prof. Dr. Marco Gercke, new ed.). Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

ITU. (2016).Definition of cybersecurity. Retrieved from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jackson, L. A., Ervin, K. S., Gardner, P. D., & Schmitt, N. (2001). Gender and the Internet: Women communicating and men searching. *Sex Roles, 44*(5), 363-379. doi:10.1023/A:1010937901821

Jay, G. M., & Willis, S. L. (1992). Influence of direct computer experience on older adults' attitudes toward computers. *Journals of Gerontology, 47*(4), 250-257.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*(2), 177-192.

Jones, C. W. (2005). *Council of Europe convention on cybercrime: Themes and critique*. Berkeley, CA: University of California at Berkeley.

Jones, S. (2002). *The Internet goes to college: How students are living in the future with today's technology*. Retrieved from http://www.pewInternet.org/files/old-media/Files/Reports/2002/PIP_College_Report.pdf.pdf

Kabay, M. E. (2008). *A brief history of computer crime: An introduction for students*. Norwich, CT: School of Graduate Studies. Retrieved from www.mekabay.com/overviews/history.pdf

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154. http://dx.doi.org/10.1016/S0268-4012(02)00105-6

Karnow, C. E. A. (1994). Recombinant culture: Crime in the digital network. Retrieved from http://cpsr.org/prevsite/cpsr/privacy/crime/karnow.html/

Kissel, R. (Ed.). (2013, May). Glossary of key information security terms (NISTIR 7298 rev. 2). http://dx.doi.org/10.6028/NIST.IR.7298r2

Kominski, R. (1992). *Computer use in the United States: The bureau of the census surveys*. Paper presented at the Annual Meeting of the American Society for Information Science, Pittsburgh, PA.

Kominski, R., & Newburger, E. (1999). *Access denied: Changes in computer ownership and use: 1984-1997*. Paper presented at the Annual Meeting of the American Sociological Association, Chicago, IL.

Kumar, A. P. (2009). *Cyber law: A view to social security*. Bangalore, India: .

Kutluca, T. (2011). A study on computer usage and attitudes toward computers of prospective preschool teacher. *International Journal on New Trends in Education and Their Implications, 2*(1), 1-17. Retrieved from http://ijonte.org/FileUpload/ks63207/File/tumu.pdf

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*, 353-363. doi:10.1016/j.dss.2011.09.002

Leary, M. R. (1995). *Introduction to behavioral research methods* (2nd ed.). Pacific Grove, CA: Brooks/Cole Publishing Company.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security, 10*(2), 57-63. http://dx.doi.org/10.1108/09685220210424104

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management, 41*(6), 707-718. http://dx.doi.org/10.1016/j.im.2003.08.008

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191-204. http://dx.doi.org/10.1016/S0378-7206(01)00143-4

Levin, T., & Gordon, C. (1989). Effect of gender and computer experiences on attitudes toward computers. *Journal of Educational Computing Research, 5*(1), 69-88. doi:10.2190/VEPG-500C-2AWM-1K15

Levy, P. S., & Lemeshow, S. (1999). *Sampling of populations: Methods and applications* (3rd ed.). New York: John Wiley and Sons.

Lewis, J. L., & Sheppard, S. R. J. (2006). Culture and communication: Can landscape visualization improve forest management consultation with indigenous communities? *Landscape and Urban Planning, 77*(3), 291-313. http://dx.doi.org/10.1016/j.landurbplan.2005.04.004

Lieberman, M. D., & Cunningham, W. A. (2009). Tools of the trade type I and type II error concerns in fMRI research: Re-balancing the scale. *Social Cognitive and Affective Neuroscience,* 4(4), 423-428. doi:10.1093/scan/nsp052

Liska, A. (1987). *Perspectives on crime and deviance* (2nd ed.). Englewood Cliffs, NJ: Prentice-Hall.

Littman, J. (1995). *The fugitive game: Online with Kevin Mitnick*. Toronto: Little Brown & Company.

Lo, C.-C., & Chen, W.-J. (2012). A hybrid information security risk assessment procedure considering interdependence between controls. *Expert Systems with Applications, 39*(1), 247-257. http://dx.doi.org/10.1016/j.eswa.2011.07.015

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186. Retrieved from http://www.jstor.org/stable/249574

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computer & Security, 24*(5), 371-380. http://dx.doi.org/10.1016/j.cose.2004.10.003

Marsh, C. (1982). *The survey method: The contribution of surveys to sociological explanation*. London: Allen & Unwin.

McHugh, J. A. M., & Deek, F. P. (2005). An incentive system for reducing malware attacks. *Communication of the ACM, 48*(6), 94-99. http://dx.doi.org/10.1145/1064830.1064833

McIlroy, D., Bunting, B., Tierney, K., & Gordon, M. (2001). The relation of gender and background experience to self-reported computing anxieties and cognitions. *Computers in Human Behavior, 17*(1), 21-33. http://dx.doi.org/10.1016/S0747-5632(00)00037-6

McIntyre, L. J. (1999). *The practical skeptic: Core concepts in sociology.* Mountain View, CA: Mayfield Publishing Company.

McLaughlin, G. (1978). Computer crime: The Ribicoff Amendment to United States code, title 18. *Criminal Justice Journal, 2*(2), 217-238.

Messner, S. F., & Rosenfeld, R. (1994). *Crime and the American dream*. Belmont, CA: Wadsworth Publishing Company.

Miller, A. R. (1971). *The assault on privacy-computers, data banks, and dossiers*. Ann Arbor, MI: University of Michigan Press.

Min, H., Lim, Y. K., & Park, J. W. (2015). Integrating X-ray technologies with intelligent transportation systems for enhancing the international maritime security. *International Journal of Logistics Systems and Management, 22*, 1-14. doi:10.1504/IJLSM.2015.070888

Mitchell, V. L., & Nault, B. R. (2003). *The emergence of functional knowledge in sociotechnical systems*. Calgary, Alberta, Canada: Haskayne School of Business University of Calgary.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. New York: John Wiley and Sons Inc.

Moeller, L., & Valentinov, V. (2012). The commercialization of the nonprofit sector: A general systems theory perspective. *Systemic Practice & Action Research, 25*(4), 365-370. doi:10.1007/s11213-011-9226-4

Moore, D. (1987). Political campaigns and the knowledge-gap hypothesis. *Public Opinion Quarterly, 51*(2), 186-200.

Morahan-Martin, J. (1998). Males, females, and the Internet. In J. Gackenbach (Ed.), *Psychology and the Internet* (pp. 169-197). San Diego: Academic Press.

Musil, S. (2014, February 19). Data breach at University of Maryland exposes 300K records. *CNET.* Retrieved from http://www.cnet.com/news/data-breach-at-university-of-maryland-exposes-300k-records

Nair, S. N., Lee, C. C., & Czaja, S. J. (2005). Older adults and attitudes toward computers: have they changed with recent advances in technology? *Proceedings of the 49th Annual Meeting of the Human Factors and Ergonomics Society* (pp. 154-157). Santa Monica, CA.

National Telecommunications and Information Administration [NTIA]. (1999). *Falling through the net: Defining the digital divide*. Washington, DC: U.S. Department of Commerce.

Neufeldt, V., & Guralnik, D. B. (1991). *Webster's new world dictionary of American English* (3rd ed.). New York: Prentice Hall.

Neumann, P. (1999, August). *The challenges of insider misuse*. Paper presented at the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse, Santa Monica, CA. Retrieved from http://www.csl.sri.com/users/neumann/pgn-misuse.html

Newman, G. R. (2009). Cybercrime. In M. D. Krohn, A. J. Lizotte, & G. Penly Hall. (Eds.), *Handbook on crime and deviance* (pp. 551-584). New York: Springer.

Nhan, J., & Bachmann, M. (2011). Developments in cyber criminology. In M. Maguire & D. Okada (Eds), *Critical issues in crime and justice: Thought, policy, and practice* (pp. 164-183). Los Angeles: SAGE.

Nhara, W. G. (1996, February). *Early warning and conflict in Africa* (OAU occasional paper no. 1). Retrieved from https://issafrica.s3.amazonaws.com/site/uploads/paper1.pdf

NIST. (1993, May). *People: An important asset in computer security* [NIST-CSL bulletin]. Retrieved from ftp://ciac.org/pub/ciac/secdocs/nist/csl93-10.txt

NIST. (2011). 2010 Computer security division 2010 annual report. Retrieved from http://csrc.nist.gov/publications/nistir/ir7751/nistir-7751_2010-csd-annual-report.pdf

NIST. (2016). *National Institute of Standards and Technology risk management framework (RMF) overview*. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/framework.html#footnote2

Nolan, J. M., Schultz, P. W., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2008). Normative social influence is underdetected. *Personality and Social Psychology Bulletin, 34*(7), 913-923. doi:10.1177/0146167208316691

Norris, P. (2001). *Digital divide: civic engagement, information poverty and the Internet in democratic societies*. New York: Cambridge University Press.

Nycum, S. H. (1976). *The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse*. Menlo Park, CA: Stanford Research Institute.

Ono, H., & Zavodny, M. (2003). Gender and the Internet. *Social Science Quarterly, 84*(1) 111-121. http://www.jstor.org/stable/42955858

Orgill, G. L., Romney, G. W., Bailey, M., & Orgill, P. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th Conference on Information Technology Education* (pp. 177-181). http://dx.doi.org/10.1145/1029533.1029577

Palis, C. (2012). Internet economy: How essential is the Internet to the U.S.? (INFOGRAPHIC) *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/2012/03/20/Internet-economy-infographic_n_1363592.html

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information.* New York: John Wiley and Sons.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAISQ). *Computers & Security, 42*, 165-176.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*, 117-129. doi:10.1177/1555343415575152

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management & Computer Security, 15*(5), 362-371. http://dx.doi.org/10.1108/09685220710831107

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757-778.

Pfohl, S. (1994). *Images of deviance and social control: A sociological history* (2nd ed.). New York: McGraw-Hill.

Pfuhl, E. H., & Henry, S. (1993). *The deviance process* (3rd ed.). New York: Aldine de Gruyter.

Pidd, M. (2003). *Tools for thinking: Modelling management science* (2nd ed.). Chichester, UK: John Wiley & Sons Ltd.

Ponemon Institute. (2013, May). *Cost of data breach study: Global analysis* (Benchmark research sponsored by Symantec and independently conducted by Ponemon Institute). Retrieved from http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

Ponemon Institute. (2014, May). *Cost of data breach study: United States* (Benchmark research sponsored by IBM and independently conducted by Ponemon Institute). Retrieved from http://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=b752a3d1-3dc2-4fa7-9cbf-d81dd8e5fcf5

Power, R. (2002). 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends 8*(1), 1-24.

Price Waterhouse Cooper. (2013). *2013 information security breaches survey*. Retrieved from www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

Posthumus, A., & von Solms, R. (2004). A framework for the governance of information security. *Computers and Security, 23*(8), 638-646. http://dx.doi.org/10.1016/j.cose.2004.10.006

Power, R. (2002). 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends 8*(1), 1-24.

Rasch, M. D. (1996). Criminal law and the Internet. In J. F. Ruh (Ed.), *The Internet and business: A lawyer's guide to the emerging legal issues*. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html

Rasmussen, J. (1994). Risk management, adaption, and design for safety. In B. Brehmer & N.-E. Sahlin (Eds.), *Future risks and risk management* (pp. 1-36). Dordrecht: Kluwer Academic Publishers.

Reason, J. (1997). *Managing the risks of organizational accidents*. Burlington, VT: Ashgate.

Reinard, J. C. (1998). *Introduction to communication research* (2nd ed.). Boston: McGraw Hill.

Resolution 45 (2006, March). *Mechanisms for enhancing cooperation on cybersecurity, including combating spam* (Document 116[Rev.5]-E). Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf

Resolution 64/211. (2009, December 21). Creation of a global culture of cybersecurityand taking stock of national efforts to protect critical information infrastructure. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol =A/RES/64/211

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Journal of Computer and Security*, *27*(1), 241-253.

Rezmierski, V. E., Seese, M. R., Jr., & St. Clair, N., II. (2002). University systems security logging: who is doing it and how far can they go? *Computers and Security*, *21*(6), 557-564. http://dx.doi.org/10.1016/S0167-4048(02)01015-5

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security*, *28*(8), 816-826. http://dx.doi.org/10.1016/j.cose.2009.05.008

Robson, C. (1993). *Real world research. A resource for social scientists and practitioner-researchers*. Oxford, UK: Blackwell.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York: Free Press.

Rogers, W. A., Cabrera, E. F., Walker, N., Gilbert, D. K., & Fisk, A. D. (1996). A survey of automatic teller machine usage across the adult life span. *Human Factors, 38*(1), 156-166.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74-104. doi:10.1111/jels.12035

Rossi, P. H., Wright, J. D., & Anderson, A. B. (Eds.). (1983). *Handbook of survey research*. New York: Academic Press.

Ryan, J. J. C. H., Mazzuchi, A. T., Ryan, J. D., Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research, 39*(4), 774-784. doi:10.1016/j.cor.2010.11.013

Salant, P., & Dillman, D. A. (1994). *How to conduct your own survey*. New York: John Wiley and Sons.

Saracho, O. N. (2013). Writing research articles for publication in early childhood education. *Early Childhood Education Journal, 41*, 45-54. doi:10.1007/s10643-012-0564-3

Sarbanes-Oxley Act of 2002, H.R.3763. (2002). Retrieved from http://beta.congress.gov/107/plaws/pub1204/PLAW-107pub1204.pdf

Sasse, M. A., & Flechais, I. (2005). Usable security. In L. F. Cranor & S. Garfinkel (Eds.), *Security and usability: Designing secure systems that people can use* (pp. 13-30). Sebastopol, CA: O'Reilly.

Schjolberg, S. (2004). Computer-related Offences. Presented at the Octopus Interface 2004 – Conference on the Challenge of Cybercrime, Strasbourg, France. Retrieved from www.cybercrimelaw.net/documents/Strasbourg.pdf

Schjolberg, S. (2008). ITU global cybersecurity agenda (GCA) (Report of the Chairman of HLEG). Retrieved from http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

Schjolberg, S., & Hubbard, A. M. (2005, June 10). *Harmonizing national legal approaches on cybercrime* (Document CYB/04). WSIS Thematic Meeting on Cybersecurity. Retrieved from https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

Schmidt, H. (2010, July 14). Progress report on cybersecurity [Blog post]. Retrieved from http://www.whitehouse.gov/blog/2010/07/14/progress-reportcybersecurity?utm_source=related

Schmidt, H. (2010, July 14). Progress report on cybersecurity. Retrieved from https://www.whitehouse.gov/blog/2010/07/14/progress-report-cybersecurity

Schneberger, S., & Wade, M. (2008). Socio-technical theory. In M. Gupta & R. Sharman (Eds.), *Handbook of research on social and organizational liabilities in information security*. New York: State University of New York.

Schneier B. (2000, October 15). Semantic attacks: The third wave of network attacks [Newsletter]. Retrieved from http://www.schneier.com/crypto-gram-0010.html#1

Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. *Journal of Organizational and End User Computing, 16*(3).

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526-531. http://dx.doi.org/10.1016/S0167-4048(02)01009-X

Schultz, E. (2005). The human factor in security. *Computers and Security*, *24*(6), 425-426.

Schultz, E. E., Proctor, R.W., Lien, M.-C., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers and Security*, *20*(18), 620-634. http://dx.doi.org/10.1016/S0167-4048(01)00712-X

Schumacher, P., & Morahan-Martin, J. (2001). Gender, Internet and computer attitudes and experiences. *Computers in Human Behavior, 17*(1), 95-110. http://dx.doi.org/10.1016/S0747-5632(00)00032-7

Schwartz, E. (1996). *Netactivism: How citizens use the Internet*. Sebastopol, CA: Songline Studies.

Schwartz, J. (1988). The computer market. *American demographics, 10*, 38-41.

Segev, A., Porra, J., & Roldan, M. (1998). Internet security and the case of Bank of America. *Communications of the ACM, 41*(10), 81-87. http://dx.doi.org/10.1145/286238.286251

Senders, J., & Moray, N. (1991). *Human error: Cause, prediction and reduction.* Hillsdale, NJ: La/Vrencc Erlbaum Associates, Inc.

Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS Quarterly, 37*(2), 565-590. Retrieved from http://misq.org/

Shappell, S., & Wiegmann, D. (2001, February). Applying reason: The human factors analysis and classification system (HFACS). *Human Factors and Aerospace Safety, 1*, 59-86.

Shashaani, L. (1993). Gender-based differences in attitudes toward computers. *Computers and Education, 20*(2), 169-181.

Shashaani, L. (1994). Gender-differences in computer experience and its influence on computer attitudes. *Journal of Educational Computing Research, 11*(4), 347-367. doi:10.2190/64MD-HTKW-PDXV-RD62

Shashaani, L. (1997). Gender differences in computer attitudes and use among college students. *Journal of Educational Computing Research, 16*(1), 37-51. doi:10.2190/Y8U7-AMMA-WQUT-R512

Shaw, R., Chen, C., Harris, A., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers and Education, 52*(1), 92-100. http://dx.doi.org/10.1016/j.compedu.2008.06.011

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1998). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications in future research. *Journal of Consumer Research, 15*(3), 325-343. http://www.jstor.org/stable/2489467

Sherman, R. C., End, C., Kraan, E., Cole, A., Campbell, J., Birchmeier, Z., & Klausner, J. (2000). The Internet gender gap among college students: Forgotten but not gone. *CyberPsychology & Behavior, 3*(5), 885-894. doi:10.1089/10949310050191854

Sieber, U. (2004, December). *Organized crime situation report: Focus on the threat of cybercrime*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf

Siegel, L. J. (1992). *Criminology: Theories, patterns, and typologies* (4th ed.). St. Paul, MN: West Publishing.

Siegel, L. J. (2006). *Criminology* (9th ed.). Belmont, CA: Thomson Wadsworth.

Simon, M., & Slay, J. (2006). Voice over IP: Forensic computing implications. Paper presented at the Australian Digital Forensics Conference. http://dx.doi.org/10.4225/75/57b13904c7058

Siponen, M. T., & Iivari, J. (2006). IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M. T., & Willison, R. (2007). *A critical assessment of IS security research between 1990-2004*. ECIS 2007 Proceedings, Paper 190. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=ecis2007

Smith, A. (2014). *Older adults and technology use*. Washington, DC: Pew Research Centre.

Smith, B., Caputi, P., & Rawstone, P. (2000). Differentiating computer experience and attitudes towards computers: An empirical investigation. *Computers in Human Behavior, 16*(1), 59-81. http://dx.doi.org/10.1016/S0747-5632(99)00052-7

Smith, M. (1989). Computer security threats, vulnerabilities and countermeasures. *Information Age, 11*(4), 205-210.

Smith, S. D. (1986). Relationships of computer attitudes to sex, grade-level, and teacher influence. *Education, 106*(3), 338-344.

Snow, G. (2011, March 31). *The 21st cntury Threat.* CyberFutures Conference, National Harbor, MD.

Sofaer, A., & Goodman, S. E. (2001). *The transnational dimension of cybercrime*. Stanford, CA: Hoover Institute Press.

Soo Hoo, K. J. (2000). *How much is enough: A risk management approach to computer security*. Working paper, Center for International Security and Cooperation, Stanford University, Stanford, CA. Available from http://cisac.fsi.stanford.edu /publications/how_much_is_enough__a_riskmanagement_approach_to_computer _security

Sproull, L., & Kiesler, S. (1992). *Connections: New ways of working in the networked organization*. Cambridge, MA: MIT Press.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 24*(2), 124-133. http://dx.doi.org/10.1016/j.cose.2004.07.001

Sterling, B. (1992). *The hacker crackdown: Law and disorder on the electronic frontier*. New York: Bantam Books.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276. http://dx.doi.org/10.1287/isre.1.3.255

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469. http://dx.doi.org/10.2307/249551

Stoll, C. (1985). *The cuckoo's egg: Tracking a spy through the maze of computer espionage*. New York: Mass Market Paperback.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276. http://dx.doi.org/10.1287/isre.1.3.255

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Summers, R. C. (1997). *Secure computing: Threats and safeguards* (Vol. 5). New York: McGraw-Hill.

SuveyMonkey. (2015). Retrieved from https://www.SuveyMonkey.com

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: Novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology, 2*(1), 67-75.

Sutherland, E. H. (1947). *Principles of criminology* (4th ed.). New York: J. B. Lippincott.

Taylor, P. (1998). *Hackers: The hawks and the doves-enemies & friends*. Unpublished manuscript.

Taylor, P. J., & Nufryk, J. (2014). *CompTIA security+ (exam SYO-401)*. Rochester, NY: Logical Operations.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570. http://dx.doi.org/10.2307/249633

Thackeray, G. (1985). Computer-related crimes: An outline. *Jurimetrics Journal, 25*(3), 300-308.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484. http://dx.doi.org/10.1016/j.cose.2005.05.002

Thomson, K.-L., & von Solms, R. (2005). Information security obedience: a definition. *Computer & Security, 24*(1), 69-75. http://dx.doi.org/10.1016/j.cose.2004.10.005

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173. http://dx.doi.org/10.1108/09685229810227649

Thong, J. Y. L., Hong, W., & Tam, K.-Y. (2002). Understanding user acceptance of digital libraries: What are the roles of interface characteristics, organizational context, and individual differences? *International Journal of Human-Computer Studies, 57*(3), 215-242. http://dx.doi.org/10.1016/S1071-5819(02)91024-4

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. (2007). Information systems security and human behaviour. *Behaviour & Information Technology, 26*(2), 113-118. doi:10.1080/01449290500330299

Trochim, W. M. K. (2006). *Research methods: Knowledge base* (3rd ed.). Retrieved from http://www.socialresearchmethods.net/kb/index.php

Tsohou, A., Karyda, M., & Kokolakis, S. (2015, July). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security, 52,* 128-141. doi:10.1016/j.cose.2015.04.006

Tzu, S. (2005). *The illustrated art of war*. (S. B. Griffith, Trans.). New York: Oxford University Press.

United Nations. (2000, April). *Crime and justice: Meeting the challenges of the twenty-first century – guide for participants*. Tenth UN Congress on the Prevention of Crime and Treatment of Offenders, Vienne, Austria.April 2000 Available from https://www.asc41.com/UN_Congress/10th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/10th%20Congress.htm

United Nations. (1994). United Nations manual on the prevention and control of computer-related crime. New York: United Nations

Velasco San Martin, C. (2009). Jurisdictional aspects of cloud computing. Proceedings of the Octopus Conference on Cooperation against Cybercrime of the Council of Europe. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204. http://dx.doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly,* 27(3), 425-478.

Vijayan, J. (2010, July 29). U.S. should seek world cooperation on cyber conflict, says ex-CIA Director. *Computer World.* Retrieved from http://www.computerworld.com/article/2519677/cybercrime-hacking/u-s--should-seek-world-cooperation-on-cyber-conflict--says-ex-cia-director.html

von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Rev. ed.). New York: George Braziller.

von Bertalanffy, L., Juarrero, A., & Rubino, A. C. (2008, June 30). An introduction to "An outline of general system theory". *Emergence: Complexity & Organization, 10*, 103-123.

Vroom, C., & von Solms, R. (2004). Towards information security behavioral compliance. *Computer & Security*, *23*(3), 191-198. http://dx.doi.org/10.1016/j.cose.2004.01.012

Ward, P., & Smith, C. L. (2002). The development of access control policies for information technology systems. *Computer & Security, 21*(4), 356-337. http://dx.doi.org/10.1016/S0167-4048(02)00414-5

Warkentin, M., & Johnston, A. C. (2006). IT security governance and centralized security controls. In M. Warkentin & R. Vaughn (Eds.), *Enterprise information systems assurance and system security: Managerial and technical issues* (pp.16-24). Hershey, PA: Idea Group Publishing.

Weiser, E. B. (2000). Gender differences in Internet use patterns and Internet application preferences: A two-sample comparison. *CyberPsychology & Behavior, 3*(2), 167-178. doi:10.1089/109493100316012

Westin, A. F., & Baker, M. A. (1973). *Data banks in a free society: Computer, record-keeping, and privacy* [Review of the book by the same title]. *Administrative Science Quarterly, 18*(3), 419-422. doi:10.2307/2391684

White, S. (2014, October 8). Global cyberattacks rose 48% in 2014. *The Journal of Accountancy.* Retrieved from www.journalofaccountancy.com/News/201411089.htm

Whitman, M. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95. http://dx.doi.org/10.1145/859670.859675

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Boston, MA: Thomson Course Technology.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Boston, MA: Course Technology Press.

Wiegmann, D., Rich, A., & Shappell, S. (2000). *Human error and accident causation theories frameworks and analytical techniques: An annotated bibliography* (Tech. rep. ARL-00-12/FAA-00-7). Savoy, IL: University of Illinois, Aviation Research Lab.

Wilson, C. (2007). *Cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. Retrieved from https://www.fas.org/sgp/crs/terror/RL32114.pdf

Wilson, J. (2010). Essentials of business research: A guide to doing your research project. Los Angeles: SAGE Publications.

Witt, K. J. (1998). Best practices in interviewing via the Internet. Proceedings of Sawtooth Software Conference, Sawtooth Software, Inc., Sequim, Washington, 15-37.

Wolfradt, U., & Doll, J. (2001). Motives of adolescents to use the Internet as a function of personality traits, personal and social factors. *Journal of Educational Computing Research, 24*(1), 13-27. doi:10.2190/ANPM-LN97-AUT2-D2EJ

Woon, I. M., & Kankanhalli, A. (2003, December). Measuring factors that influence information security effectiveness in organizations. *Proceedings of the 13th Annual Workshop on Information Technologies and Systems* (pp. 19-24). Seattle, WA.

Yee, H. E. (1984). Juvenile computer crime—hacking: Criminal and civil liability. *Communications and Entertainment Law Journal, 7*, 335.

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yoh, E., Damhorst, M. L., Sapp, S., & Laczniak, R. (2003). Consumer adoption of the Internet: The case of apparel shopping. *Psychology & Marketing, 20*(12), 1095-1118. doi:10.1002/mar.10110

Yushau, B. (2006). The effects of blended e-learning on mathematics and computer attitudes in pre-calculus algebra. *The Montana Mathematics Enthusiast, 3*(2), 176-183. Retrieved from http://www.math.umt.edu/tmme/vol3no2/TMMEvol3no2_SaudiArabia_pp176_183.pdf

Zeithaml, V. A., & Gilly, M. C. (1987). Characteristics affecting the acceptance of retailing technologies: A comparison of elderly and nonelderly consumers. *Journal of Retailing, 63*(1), 49-68.

Zhang, X., van Donk, P. D., & van der Vaart, T. (2011). Does ICT influence supply chain management and performance? A review of survey-based research. *International Journal of Operations & Production Management, 31,* 1215-1247. http://dx.doi.org/10.1108/01443571111178501

Zickuhr, K. (2013). *Who's not online and why* [Report]. Available from http://www.pewInternet.org/2013/09/25/whos-not-online-and-why/